STEGANOGRAPHIC APPROACH BASED ON COMPUTER GAME

Krasimir M. Kordov, Daniel E. Yordanov

ABSTRACT: *In this paper we present untraditional steganographic approach for hiding secret information in one of the most famous classical game. Using a game as stegocontainer defines different method for steganography considering the game structure and different method for using steganographic key. Further more the visual steganographic analysis is provided to demonstrate the necessary level of security of the proposed steganographic method.*

KEYWORDS: *Steganography, Steganographic approach, Computer game*

СТЕГАНОГРАФСКИ ПОДХОД, БАЗИРАН НА КОМПЮТЪРНА ИГРА*

Красимир М. Кордов, Даниел Е. Йорданов

1 Въведение в стеганографията

Стеганологията е научно направление, което се състои от две подразделения - Стеганография и Стегоанализ (Стеганализ или Стеганографски анализ) [2, 3, 7, 16, 22]. Стеганографията има за цел разработването на методи, модели и алгоритми за скриване на тайна информация, докато стегоанализът има за цел разкриването на приложена стеганография [23]. Разкриването на самата скрита информация не е обект на стеганализа, но се счита, че стеганографският подход е неуспешен, ако стеганализът отчете наличие на скрита информация [5, 6, 21].

В миналото, информацията [1] се е пренасяла основно под формата на текст, а стеганографията се използва, за да се скрие текст по такъв начин, че единствено очаквания получател да знае за съществуването на скрит текст [4]. В днешни дни, компютърните технологии позволяват пренос на информация, базирана на цифрови и аналогови сигнали, като преносимата информация е многообразна – текст, изображения, аудио, видео и дори игри. В компютърните системи информацията се съхранява и предава в двоичен код и по тази причина съвременната стеганография е фокусирана върху алгоритми скриващи информация в дигитален вид [7].

Стеганографската система е множество от елементи, взаимодействащи помежду си, всяко от които оказва влияние на скритото съобщение (информация), но в последствие съобщението трябва да достигне до желания получател в оригиналният си вид. Частите на системата се наричат подсистеми и всякакви промени в тях могат да доведат до провал на стеганографията [2]. С развитието на високо технологичната стеганография [4] се наблюдава използването на криптографски способи за предаване на секретен ключ между участниците в кореспонденцията или за хаотично скриване на тайната информация. Подобни алгоритми са разгледани в [13, 19] като за целта са използвани псевдослучайни генератори на двоични числа [11, 12, 17, 18].

*Настоящата статия е частично финансирана от фонд „Научни изследвания” на Шуменски Университет „Епископ К. Преславски” по проект № РД-08-122/06.02.2018.

2 Индустрия на компютърните игри

Компютърните игри са се обособили като глобална развлекателна индустрия, популярна за хора от всички възрастови групи. Съвременното информационно общество има достъп до игри на различни платформи (смартфони, таблети, персонални компютри, игрови конзоли и др.). Развитието на компютърните технологии води до развитие и популяризиране на игри от различни категории и жанрове, като някой от най-популярните игри се използват от милиони потребители по целия свят. Огромни количества от информация се пренася на сървъри до потребители на игри (и обратно) по целия свят и потока от данни който се предава непрекъснато е огромен [14, 15]. Това създава условия за използване на стеганографско предаване на тайна информация.

Бурното развитие на компютърните игри води своето начало през 60-те години на миналият век [10, 20]. Въпреки предназначението на компютъра за изчислителни процеси, графичното представяне на информация дава възможност да се измислят игри. Това от своя страна води до производство на специализирани хардуерни конфигурации, наречени игрови конзоли (или само конзоли), предназначени изцяло за игри. За първата компютърна конзола може да се приеме машината PDP-1 (Фигура 1 - а)), на която през 1962 година е създадена играта Spacewars, която се счита за първата компютърна игра [20]. По-късно през 1972 година се появяват аркадните игри. Използвали са се специални машини (Фигура 1 - б)), широко разпространени в барове и други заведения по цял свят. Една от най-популярните игри по това време е била Pong [20]. След нейното преиздаване за домашни конзоли, те се превръща в една от първите игри „първо поколение видео игри“. Второто поколение се играе на конзоли, които позволявали да се играе повече от една видео игра.

а) PDP-1

б) Аркадна конзола

Фигура 1: Първите компютърни конзоли.

През 1983 започва т. нар. сребърна епоха на видео игрите. По това време двамата гиганти в гейм индустрията са Nintendo[24] и Sega[25]. В наши дни мястото на Nintendo и Sega е заето от PlayStation[27] и Xbox[26], които продължават войната на конзолите. Борбата за потребители води до непрекъснати подобрения в качеството на игрите и генерира огромни приходи на производителите на конзоли и игри.

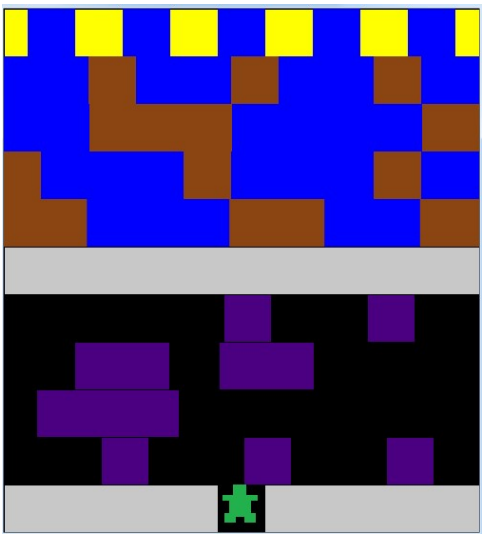
Индустрията на компютърни игри води до надпревара сред производителите на хардуер, но също така и до надпревара между производителите на игри. Съществуват компютърни компании, с хиляди специалисти, работещи изцяло върху създаването на нови игри, купува-

ни от милиони потребители по цял свят. Едни от най-известните производители на игри са Bethesda[28], Ubisoft[29], Rockstar games[30], CD Project RED[31] и други.

3 Стеганографски подход, базиран на компютърна игра

Преди идеята за скриване на информация в игри, създателите на игри са допускали грешки в разработката на своите продукти, което довежда до множество неочаквани резултати – гличове (glitches). Но не всички грешки имали лоши последици, защото някои играчи били заинтригувани и с интерес търсели други подобни необичайни елементи в игрите [8, 9]. Програмистите се възползват от това неочаквано постижение и започват да добавят скрито съдържание във своите игри, а ако има гличове, които се харесват от играчите, то тези „грешки“ не биват премахвани. Това и до ден днешен се харесва на играчите по цял свят и повишава интереса към компютърните игри. Тази практика се е превърнала в практика за предаване на тайна информация от производителите на игри към играчите, като дори се използват за рекламни послания за продукти от ежедневието в реалния свят [9].

В нашият случай, предаването на скрита информация е предназначено от един потребител до друг, като за целта е използвана собствена реализация на една от класическите аркадни игри - Frogger. Тази игра от златната епоха на видео игрите е популярна и в наши дни и по тази причина има много разновидности. Реализацията която предлагаме е направена на Java и изглежда по следният начин.



Фигура 2: Реализация на играта Frogger

3.1 Скрита функционалност на играта

Реализираната игра е опростена, с цел да се наблегне на стеганографският модел, вграден в играта. Няма нива на сложност, промяна на скоростта или допълнителни графични промени. Скритата функционалност на играта дава възможности на потребителите да обменят скрита информация, при активиране на скритата функционалност. Трябва да се изпълнят следните действия:

Стъпка 1: При натискане на конкретен бутон от клавиатурата (в нашият случай „C”) се включва режим за стеганография, като може да бъде изключен по същия начин. Реална

индикация не се визуализира с цел запазване на потайността на скритата функционалност.

Стъпка 2: Прави се избор за кодиране или декодиране на информация, като се позиционира игровия обект (frog) съответно в долният-ляв или долният-десен край на екрана.

Стъпка 3: За изпълнение на кодиране или декодиране трябва да се въведе правилен ключ. В нашият случай, това означава да се изиграе играта по точно определен начин.

Стъпка 4: След проверка на въведения ключ, в диалогов прозорец, на потребителя се предоставя възможност да въведе тайно съобщение (при режим на кодиране) или се показва тайното съобщение (при режим на декодиране).

3.2 Методи за скриване на информация

Реализацията на игра, позволява изпробването на различни методи за скриване информация. Стеганографията е реализирана по следните начини:

1) Метод на празните редове - при този метод се използват празни редове в програмния код на играта. Това по никакъв начин не променя функционалността на играта и остава скрито за потребителите. За целта всеки символ от скритото съобщение се трансформира в двоичен код, чрез своят ACSII код и в празен ред с разделители (интервали и табулатори) последователно се записват в празният ред от кода. Интервалите и табулаторите също не влияят на програмния код и на функционалността на играта.

2) Метод за добавяне на разделители - този метод отново използва преобразуване на тайното съобщение в двоичен код и скриване на информацията в програмния код на играта. Принципът на скриване е използването на разделителите (интервали и табулатори) в края на всеки ред от програмния код. Този метод избягва поява на излишни празни редове, за да не се предизвиква съмнение за стеганография, дори и при прочитане на програмния код.

3) Използване на динамичен файл - при този метод се използва файла за записване на резултатите от играта. Това е динамичен файл, в който постоянно се записват данни, което не предизвиква съмнение при стеганографски анализ.

4 Стеганографски анализ

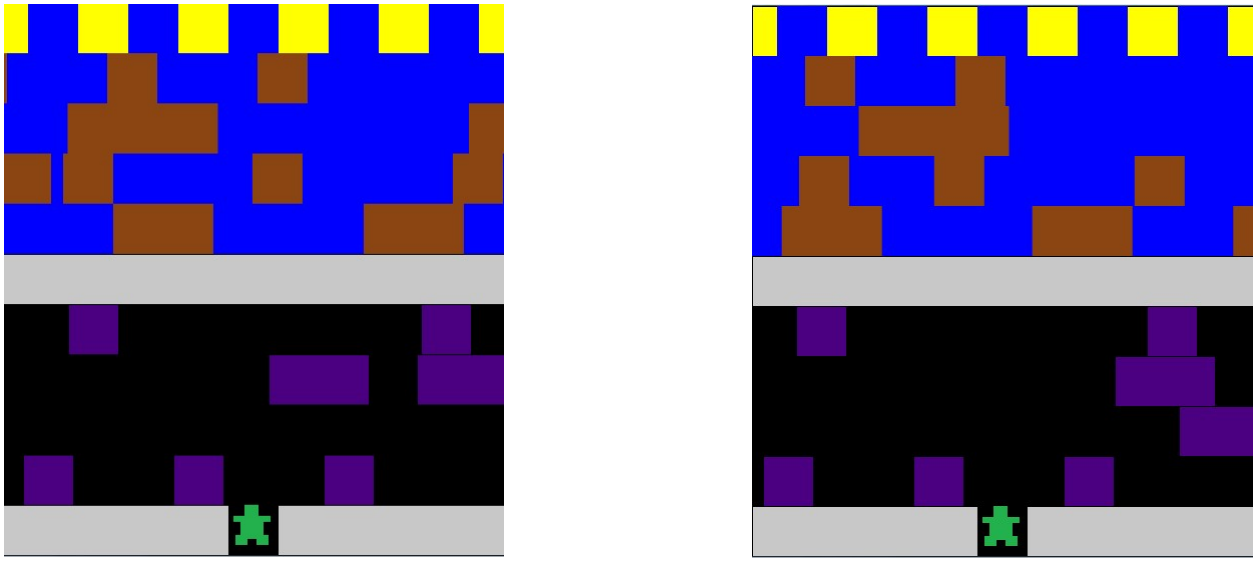
Стеганографският анализ е изследване, което има за цел да провери за наличие на стеганография. Изборът на нетрадиционен метод за скриване на тайна информация в компютърна игра, прави традиционните изследвания неприложими. По тази причина са разгледани само двата най-важни аспекта на стеганографията - визуалният анализ и чувствителността към секретния ключ.

4.1 Визуален анализ

Визуалният анализ определя наличието на видими разлики в началните условия, преди и след използването на стеганография. При предложеният метод на стеганография се прави сравнение във функционалността на играта и на програмната библиотека при скриване на тайна информация.

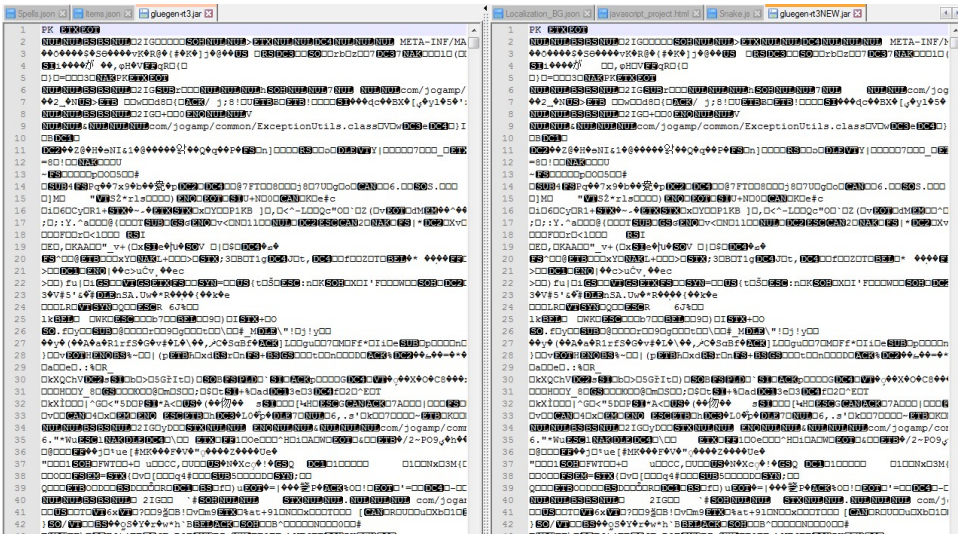
Показаният визуален анализ на (Фигура 3) нагледно показва, че няма забележима разлика във функционалността на играта, независимо дали присъства стеганография.

При сравнението на библиотечните файлове, съдържащи програмния код на играта (Фигура 4) се демонстрира невъзможност да се разчете някаква информация, поради специфичният начин на визуализиране на библиотечните файлове с програмен код на Java.



а) без скрита информация б) при скрита информация

Фигура 3: Визуален анализ - функционалност на играта.

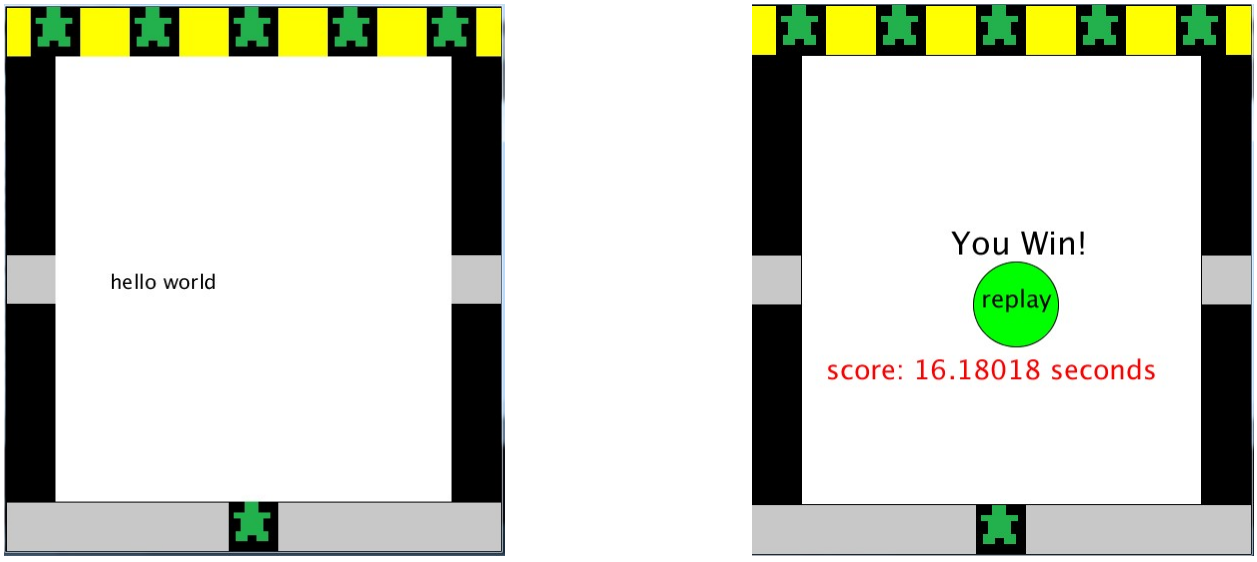


Фигура 4: Визуален анализ - сравнение на програмния код.

4.2 Чувствителност към секретният ключ

Използването на компютърна игра за скриване на информация, променя донякъде разбирането за секретен ключ, в този случай. Под секретен ключ се разбира фиксирана последователност от действия, които трябва да се извършат в играта. Играта трябва да се изиграе по точно определен, предварително зададен начин, като последователността е следната - 2, 0, 3, 1, 4. Тази последователност представлява секретния ключ на стеганографският метод. Това е изследване, което показва чувствителността към секретния ключ, като за целта се използва ключ K1 и леко променен ключ K2. Експериментите показват, че дори и при малка промяна на секретния ключ е невъзможно да се разкрие скритата информация. За експерименталното

тестване, оригиналният ключ К1 е избран с позиционна последователност 2,0,3,1,4 и ключ К2 е избран с минимална разлика - 2,0,3,4,1. На (Фигура 5) е показано, че при минимални разлики в ключа, дори самата стеганографска функционалност остава скрита.



а) секретен ключ К1 б) секретен ключ К2

Фигура 5: Чувствителност към секретния ключ.

При използване на вярна последователност (К1) играта коректно активира стеганографската функционалност, но при всички останали случаи потребителят приключва играта по стандартен начин.

5 Заключение

Компютърните игри са световен феномен в последните години и са се превърнали в едни от печелившите индустриални фактори в глобален мащаб. Те са широко разпространени, динамични (променяни, подобрявани и обновявани) и дори вече повечето игри целенасочено съдържат скрита информация с апелативна функция към потребителите, което прави скриването на допълнителна информация още по удобно и неочаквано. Подобно скриване на информация предлага много по-добра защита от други стеганографски методи, защото компютърните игри могат да предоставят огромен стегокапацитет и да бъдат хранилище за скрита информация, без това да указва влияние на качеството на самата игра.

Представеният стеганографски алгоритъм, базиран на компютърна игра демонстрира нетрадиционна стеганография на цифрова информация, а направеният стеганографски анализ, показва наличие на необходимото ниво на сигурност при използване на предложеният алгоритъм.

ЛИТЕРАТУРА:

[1] Семерджиев, Ц., (2007) Сигурност и защита на информацията. София: Класика и стил. 2007. ISBN 978-954-327-034-7.

[2] Станев, С., (2013), Стеганологична защита на информацията. Университетско издателство „Епископ Константин Преславски”. Шумен, 2013. ISBN 978-954-577-825-4. 320.

[3] Станев, С., Стоянов, Б., (2016), Предизвикателствата на стеганографията към информационната сигурност и обучението на специалисти, Годишник на ШУ „Епископ К. Преславски" Факултет по математика и информатика, том XVII С, 2016

[4] Станев, С., Железов, С., Параскевов, Х., Христов, Х., (2015), Ръководство за упражнения по стеганография, Университетско издателство „Епископ Константин Преславски", Шумен 2015.

[5] Станев, С., Железов, С., Якимов, И., (2012), Реализация на паралелен стеганализ с клъстерна система, Международна научна конференция" Съвременни методи и технологии в научните изследвания", Варна 2012.

[6] Fridrich, J., (2006), Steganalysis. In Multimedia Security Technologies for Digital Rights Management (pp. 349-381).

[7] Fridrich, J.,(2010), Steganography in Digital Media: Principles, Algorithms, and Applications. Cambridge University Press, 437 p. ISBN 978-0521190190.

[8] Gibbs, C., Shashidhar, N., (2015), StegoRogue: Steganography in Two-Dimensional Video Game Maps. Advances in Computer Science: an International Journal, 4(3), 141-146.

[9] Hale, C., Chen, L., Liu, Q., (2012, December), A new villain: Investigating steganography in source engine based video games. In Proceedings of the 2012 Hong Kong International Conference on Engineering & Applied Science (HKICEAS), Hong Kong, China, December 14 (Vol. 16).

[10] Kent, S. L., (2010). The Ultimate History of Video Games: from Pong to Pokemon and beyond... the story behind the craze that touched our lives and changed the world. Three Rivers Press.

[11] Kordov, K., (2014), Modified Chebyshev Map Based Pseudo-random Bit Generator. In AIP Conference Proceedings (Vol. 1629, pp. 432-436).

[12] Kordov, K., (2015), Signature Attractor Based Pseudorandom Generation Algorithm. Advanced Studies in Theoretical Physics, 9(6), 287-293.

[13] Kordov, K., Stoyanov, B., (2017), Least Significant Bit Steganography using Hitzl-Zele Chaotic Map, International Journal of Electronics and Telecommunications, 63(4), 417-422. doi: https://doi.org/10.1515/eletel-2017-0061

[14] Marchand, A., Hennig-Thurau, T., (2013), Value creation in the video game industry: Industry economics, consumer benefits, and research opportunities. Journal of Interactive Marketing, 27(3), 141-157.

[15] Novak, J., (2011), Game development essentials: an introduction, Cengage Learning.

[16] Stanev, S., Szczypiorski, K., (2016), Steganography Training: a Case Study from University of Shumen in Bulgaria, International Journal of Electronics and Telecommunications, 62(3), 315-318. doi: https://doi.org/10.1515/eletel-2016-0043

[17] Stoyanov, B., (2014), Pseudo-random Bit Generation Algorithm Based on Chebyshev Polynomial and Tinkerbell Map. Applied Mathematical Sciences, 8(125), 6205-6210.

[18] Stoyanov, B., (2014, November), Using circle map in pseudorandom bit generation. In AIP Conference Proceedings (Vol. 1629, No. 1, pp. 460-463). AIP.

[19] Stoyanov, B., Zhelezov, S, Kordov, K., (2016), Least significant bit image steganography algorithm based on chaotic rotation equations, Comptes rendus de l'Académie bulgare des Sciences, 69(7), 845-850.

[20] Wolf, M. J. (Ed.). (2008). The video game explosion: a history from PONG to Playstation and beyond. ABC-CLIO.

[21] Zhelezov, S., (2016), Modified Algorithm for Steganalysis, Mathematical and Software Engineering, 1(2), 31-36.

[22] Zhelezov S., Paraskevov H., (2015), Possibilities for steganographic parallel processing with a cluster system, Contemporary Engineering Sciences, 8(20).

[23] Zielińska, E., Mazurczyk, W., Szczypiorski, K., (2014)., Trends in steganography. Communications of the ACM, 57(3), 86-95.

[24] URL: https://www.nintendo.com/ - официален сайт на Nintendo (20.06.2018).

[25] URL: http://www.sega.com/ - официален сайт на Sega (20.06.2018)

[26] URL: https://www.xbox.com/ - официален сайт на XBOX (20.06.2018)

[27] URL: https://www.playstation.com/ - официален сайт на Playstation (20.06.2018)

[28] URL: https://bethesda.net/ - официален сайт на Bethesda (20.06.2018)

[29] URL: https://www.ubisoft.com/en-gb/ - официален сайт на Ubisoft (20.06.2018)

[30] URL: https://www.rockstargames.com/ - официален сайт на Rockstar games (20.06.2018)

[31] URL: http://en.cdprojektred.com/ - официален сайт на CD Project RED (20.06.2018)

Красимир Кордов, Даниел Йорданов
Шуменски университет ”Еп. Константин Преславски”
E-mail: krasimir.kordov@shu.bg

MOBILE APPLICATION FOR ORDER MANAGEMENT

Krasimir M. Kordov, Bilnur V. Islyam

ABSTRACT: *In this paper we present mobile software for order management using MIT App Inventor for Android applications. The application is designed to optimize traditional method for making order allowing business to save time and expenses by making the clients to select and order products using mobile devices.*

KEYWORDS: *Mobile application, Mobile software, MIT App Inventor*

МОБИЛЕН СОФТУЕР ЗА УПРАВЛЕНИЕ НА ПОРЪЧКИ*

Красимир М. Кордов, Билнур В. Ислям

1 Увод

Мобилните устройства заемат все по-голям пазарен дял с всяка изминала година, като постепенно изместват персоналните компютри. Надпреварата между производителите на мобилни устройства прави достъпни за потребителите смартфони и таблети с изчислителна мощ на персонален компютър на все по-ниски цени. В световен мащаб почти няма дом, в който да не присъства поне един таблет или телефон [2].

Наличието на огромният брой мобилни устройства, използвани от потребителите оказва влияние и върху разработчиците на софтуер, които трябва да се съобразяват с платформите, които използват потребителите. В последните години се разработват мобилни приложения за всички сфери на реалния живот – бизнес приложения, игри, приложения за банкиране, плащане на сметки, приложения за електронна търговия и др. Някои от мобилните приложения са толкова популярни, че достигат до няколко милиарда изтегляния. Това показва интереса на потребителите към мобилните приложения. Разработването на мобилни приложения може да носи значителни печалби на разработчиците им, затова в този бранш непрекъснато се включват нови участници от обикновени програмисти до компании, които са софтуерни гиганти на световния пазар [1, 4].

2 Мобилни устройства

Мобилните устройства най-общо се разделят на смартфони и таблети, като те са лесно преносими (мобилни), заради малките си размери. Основната разлика е, че смартфоните, задължително предлагат възможност за мобилни услуги (разговори чрез мобилен оператор, трансфер на данни и др.), докато при таблетите това условие не е задължително. Друга разлика е в размерите на устройствата, като таблетите често са малко по-големи от смартфоните, но въпреки това достатъчно малки и удобни за използване и пренасяне.

*Настоящата статия е частично финансирана от фонд „Научни изследвания” на Шуменски Университет „Епископ К. Преславски” по проект № РД-08-122/06.02.2018.

2.1 Развитие на мобилните устройства

През 1973 година компанията MOTOROLA изобретява първият мобилен телефон, но през 90-те години на миналия век, клетъчните телефони влизат в масова употреба [2]. Паралелно с развитието на мобилните телефони се развиват компютрите, като тяхната изчислителна мощ нараства с изключително бързи темпове, докато размерите на компютърните компоненти стават все по-малки. През втората половина на 90-те години тези технологии се преплитат и мобилните телефони вече притежават функциите на малки джобни персонални компютри, използвани за комуникация. Тези устройства имат операционна система, което позволява да се инсталират допълнителни приложения и така да се разширят възможностите на мобилните телефони [4]. Терминът смартфон започва да се използва през 2000 година от шведският производител на мобилни телефони Ericsson. Смартфоните са следващата стъпка в еволюцията на мобилните телефони, но съществената разлика е, че смартфоните притежават всички функции на мобилен телефон, но и допълни възможности за обработка на данни, което е характерно за персоналните компютри. Основните характеристики на смартфоните са:

- наличие на достатъчно развита операционна система
- липса на хардуерна клавиатура
- наличие на сензорен дисплей
- възможност за инсталиране на допълнителен софтуер (мобилни приложения)
- възможност за използване на мобилни услуги
- възможност за използване на Интернет

На Фигура 1 са показани примери за съвременните смартфони.

Фигура 1: Смартфони

Таблетите се появяват на пазара през 2000 година, като наследник на Tablet PC въведен от компанията Microsoft. Този вид мобилно устройство е проектирано, като алтернатива на лаптопите и притежава собствен процесор и операционна система. Удобството за работа с таблети, бързо налага на пазара този вид мобилни устройства. Някои модели таблети са с разширени функции, за да могат да се използват и като смартфони. По-важните характеристики на таблетите са:

- наличие на достатъчно развита операционна система

- липса на хардуерна клавиатура
- наличие на сензорен дисплей
- възможност за инсталиране на допълнителен софтуер (мобилни приложения)
- някои модели имат възможност за използване на мобилни услуги
- възможност за използване на Интернет
- притежават по-голям дисплей от смартфоните
- по-удобни са от смартфоните при четене на текстове, гледане на видео съдържание и въвеждане на текст

На Фигура 2 са показани примери за съвременни таблети:

Фигура 2: Таблети

2.2 Операционни системи за мобилни устройства

Разработването на мобилни приложения е свързано с операционната система, инсталирана на мобилното устройство. Въпреки наличието на милиони мобилни приложения, техните разработчици винаги се съобразяват с операционната система, на която трябва „да се изпълняват“ техните приложения. Към този момент най-разпространените операционни системи са Android на компанията Google Inc., IOS на компанията Apple Inc. и Windows 10 Mobile на компанията Microsoft. Операционните системи на тези софтуерни гиганти, заедно покриват над 95% от използваните мобилни устройства в световен мащаб. Операционната система Android [5] заема най-голям пазарен дял на мобилни устройства в света, като в някои държави този дял достига впечатляващите 90%. Тази операционна система е базирана на ядрото на Linux и е разработена от софтуерната компания Android Inc., която през 2005 година е купена от софтуерният гигант Google Inc. [7]

Следващата по популярност операционна система за мобилни устройства е IOS, разработена от Apple Inc. [6] Първата версия на тази операционна система се появява заедно с първият смартфон на Apple през 2007 година. Компанията Apple Inc. е сериозен производител на хардуер и създава операционни системи които да работят конкретно и само с устройства създадени от самата компания. Това е причината IOS да не работи с хардуер на трети страни. На следващото изображение е показано първото лого на операционната система IOS.

Следващата операционна система на мобилни устройства е на друг световен софтуерен гигант Microsoft [8]. Въпреки че тази компания е лидер на пазара при операционните системи за персонални компютри, при операционните системи за мобилни устройства тя значително

отстъпва на първите две описани операционни системи. Към този момент най-актуалната версия е Windows 10 Mobile, която е наследник на Windows Phone.

На Фигура 3 са показани официалните лога на описаните мобилни операционни системи.

Фигура 3: Официални лога на Android, IOS и Windows

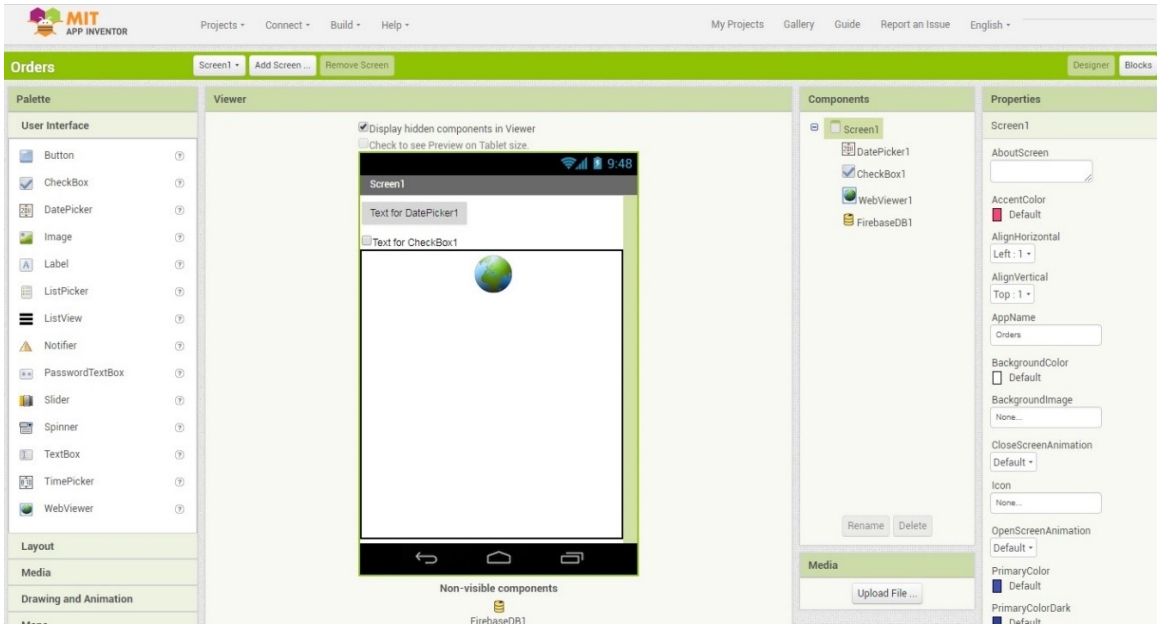
3 Мобилни приложения

Мобилното приложение представлява компютърна програма, предназначена да работи на мобилни устройства. Това означава, че мобилните приложения са софтуер, който се разработва за специфичен хардуер (смартфони и таблети). Широкото разпространение на мобилни устройства в световен мащаб е преориентирало и софтуерните производители да реализират своят софтуер и за мобилни устройства, а някои от софтуерните разработчици са изцяло ориентирани към разработването само на мобилни приложения. Към този момент съществуват милиони мобилни приложения, като тенденцията е те да се увеличават. Голяма част от мобилните приложения са безплатни или на ниски цени. Безплатните приложения се финансират от вградени в тях реклами, но както при тях така и при приложенията на ниски цени, големият брой изтегляния гарантира сериозни печалби за техните разработчици. Някои от най-популярните мобилните приложения се използват от милиони потребители, което носи огромни печалби. Мобилните приложения имат различно предназначение и могат да участват във всички аспекти на съвременното ежедневие на потребителите. Съществуват мобилни приложения за навигация, видео комуникация, социални мрежи, електронна търговия, разплащане, игри и развлечение, здраве и спорт, обучение и много други. Бизнесът от своя страна също използва мобилните приложения за връзка със своите клиенти за представяне на своите стоки и услуги, обяви, промоции, поръчки, разплащане и др. Фирмите инвестират средства за разработване на мобилни приложения за рекламиране на своята дейност и създават мобилни версии на своите web-сайтове за по удобна връзка с клиенти. Тази тенденция е изцяло продиктувана от непрекъснато увеличаващия се брой използвани мобилни устройства и лесният достъп до пазара за мобилни приложения. Разпространението на мобилни приложения най-общо се контролира от производителите на операционни системи. Операционните системи имат вградени приложения, които представляват „пазар за приложения“ [3]. Приложението за Android се нарича Google Play, приложението за IOS е App Store, а приложението за Windows Mobile е Windows Store. Потребителите получават голяма степен на сигурност използвайки тези приложения, защото всички предлагани за изтегляне приложения са предварително проверени от производителите на операционни системи.

4 MIT App Inventor

Инструментите за създаване на мобилни приложения дават възможност да се създават дизайни, програмна логика на приложения, форми, бутони и интерфейси, които се „превеж-

дат“ за да могат да работят на мобилни устройства. Те могат да съдържат шаблонни дизайни на приложения или да използват авторски дизайн и функционалност зададена от разработчиците на софтуер. Пример за инструменти за създаване на мобилни приложения е MIT App Inventor [9], използван за реализация на приложението за управление на поръчки в настоящата статия. Първоизточникът на този софтуерен продукт е App Inventor for Android създаден от Google, като web-базиран софтуер с отворен код. В момента приложението се поддържа от Масачузетския технологичен институт (MIT), а приложението се нарича MIT App Inventor. За използване на този софтуер се изисква използване на web-браузър и интернет връзка. Менютата са удобни за използване и са подредени интуитивно. Елементите, които могат да се използват в приложенията са изключително разнообразни, като изображения за дизайна, бутони за социални мрежи, мултимедийни елементи, бази от данни, карти от Google Maps, елементи използващи сензорите на устройството и др. Началният екран е показан на следващата Фигура 4.



Фигура 4: Начален екран на MIT App Inventor

5 Мобилен софтуер за управление на поръчки

5.1 Концепция на мобилното приложение

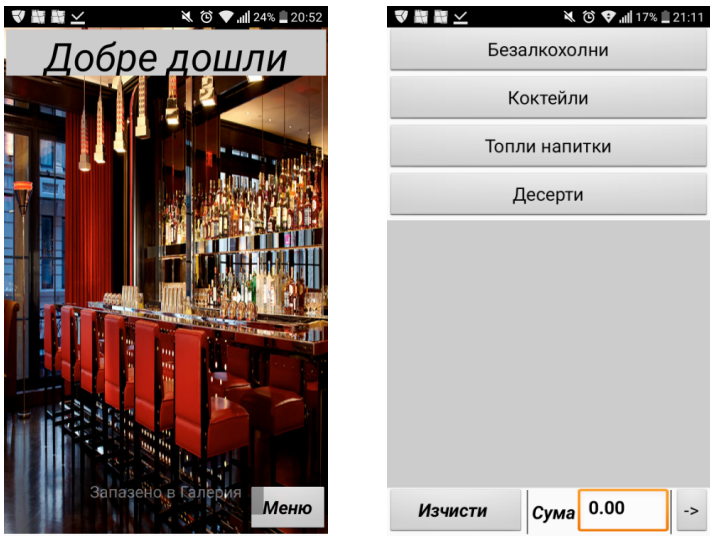
Традиционният начин за приемане на поръчки включва няколко стъпки, в които участват клиентите и служител, обслужващ съответната маса в заведението за хранене, ресторанта и др.

- Служителят предоставя на клиентите меню с продуктовия асортимент на заведението
- Клиентът избира желаните продукти
- Служителят записва желаните от клиента продукти и техният брой
- Служителят предоставя списъкът с желаните от клиента във вид на поръчка за изпълнение на барман, кухня или управител.

След тези стъпки поръчката е приета и се изпълнява от друг вид обслужващ персонал. Очевидните затруднения, които могат да възникнат е ако заведението има много клиенти за обслужване или има недостатъчно персонал. Това може да доведе до недоволни клиенти и последващи намаления на приходите. Всеки бизнес, независимо в коя сфера работи, зависи от своите клиенти, защото това пряко влияе на печалбата на фирмата. За да се улеснят клиентите е необходимо да се създават удобства за клиентите и улесняване на техния избор. Инвестицията в нови технологии може до голяма степен да постигне тази цел. Една такава нова технология може да бъде мобилен софтуер за управление на поръчки. Създаването на мобилно приложение за управление на поръчки може значително да улесни клиентите, като е необходимо да се поставят изисквания, на които да отговаря разработеният софтуер.

5.2 Реализация на мобилното приложение

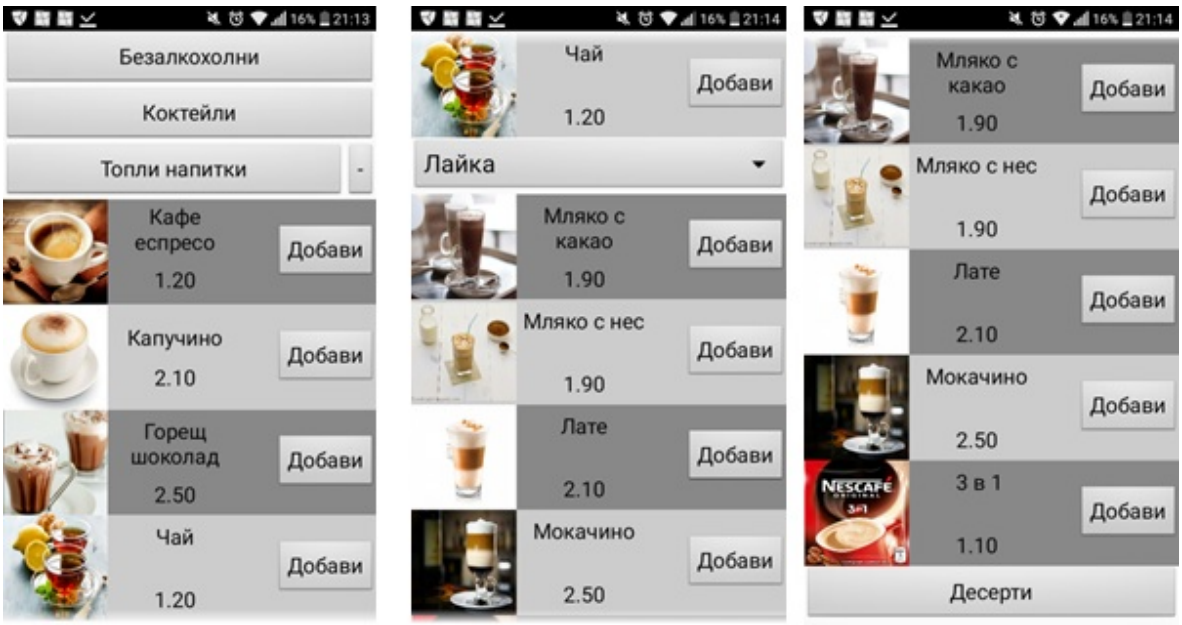
Началният екран на приложението съдържа фонова картина, която е снимка на заведението, текст, който приветства гостите и бутон ”Меню” , който при натискане препраща към менюто на заведението. На Фигура 5 е показан изгледа на началния екран на мобилното приложение.



а) начален екран б) избор на категория

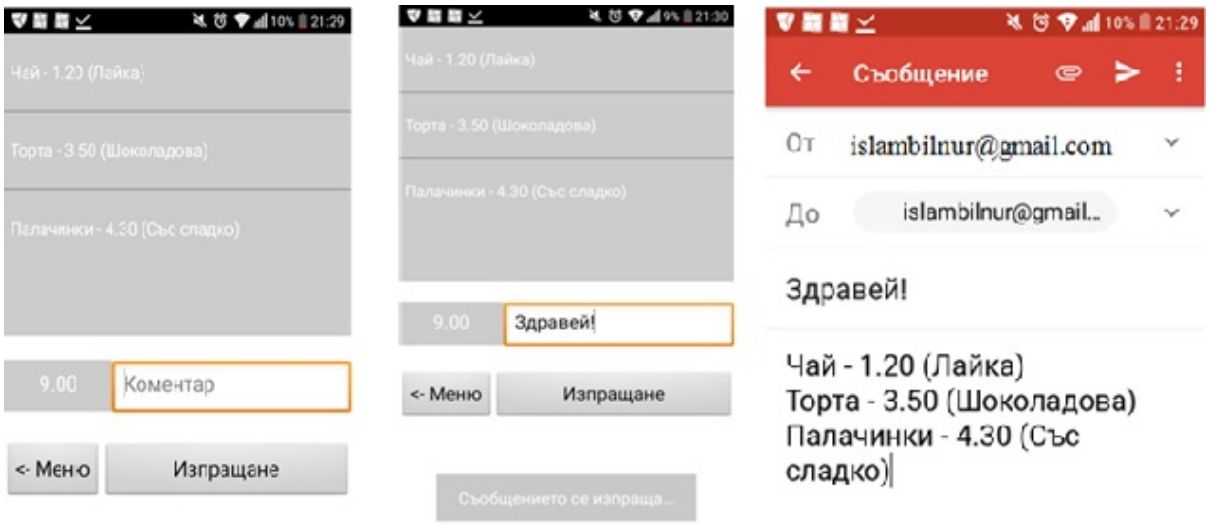
Фигура 5: Мобилно приложение

След натискане на бутон Меню, клиентите могат да се запознаят с менюто на заведението, където продуктите са разпределени в отделни категории. При избиране на съответната категория, се показват продуктите от тази категория. Има 4 категории продукти, като има възможност да се добавят още категории и продукти в менюто. Под категориите има списъчен елемент, където се показват избраните продукти от клиента. Една от категориите в приложението е показана на следващата Фигура 6.



Фигура 6: Мобилно приложение

Продуктите, които имат допълнителни разновидности, след маркиране, дават възможност на клиента да уточни желаната опция чрез падащо меню. Предвидени са ситуациите когато клиента желае да премахне продукт или да изтрие цялата поръчка. На екрана на мобилното приложение се показва диалогов прозорец за потвърждение на изтриването, в който клиента прави окончателният си избор. При избора на всеки следващ продукт приложението калкулира крайната сума на поръчката.



Фигура 7: Мобилно приложение

Последният етап на създаване на поръчка позволява на клиента да прегледа крайния

списък с избрани продукти и цената на поръчката, както и да изпрати кратко текстово съобщение.

6 Заключение

Всяка изминала година производителите на мобилни устройства отчитат все по-големи продажби, което е индикатор за броя на използваните мобилни устройства в световен мащаб. Тази конкуренция указва благоприятно влияние на пазара за мобилни устройства, като цените стават по-достъпни за потребителите, качеството на мобилните устройства се подобрява, което е довело до факта, че почти няма домакинство, в което да няма поне едно мобилно устройство. Огромният брой използвани мобилни устройства предполага бурното развитие на мобилен софтуер за тези устройства. В последните години се разработват милиони мобилни приложения и тази тенденция не подминава и бизнес средите. Дори и малкият бизнес интензивно се включва на пазара за мобилни приложения, като разработват мобилни версии на техните сайтове, приложения за комуникация със своите клиенти, каталози на продукти, приложения за пазаруване и др. Настоящата статия представя концепция и реализация за разработване на мобилен софтуер за управление на поръчки, с което се оптимизира работата на персонала в заведения за хранене, ресторанти, барове, пицарии и др. Мобилното приложение предлага удобен потребителски интерфейс, който улеснява клиентите при разглеждане на менюто на заведението и поръчките, които се приемат от централизиран компютър посредством безжична мрежа. Целта на приложението е спестяване на време и съкращаване на разходите за персонал при управлението на поръчки.

ЛИТЕРАТУРА:

[1] Agar, J., (2013). Constant touch: A global history of the mobile phone. Icon Books Ltd.

[2] Castells, M., Fernandez-Ardevol, M., Qiu, J. L., Sey, A. (2009). Mobile communication and society: A global perspective. Mit Press.

[3] Holzer, A., Ondrus, J. (2011). Mobile application market: A developer's perspective. Telematics and informatics, 28(1), 22-31.

[4] Kenney, M., Pon, B. (2011). Structuring the smartphone industry: is the mobile internet OS platform the key?. Journal of Industry, Competition and Trade, 11(3), 239-261

[5] URL: https://www.android.com/ - официален сайт на Android (20.08.2018).

[6] URL: https://www.apple.com/ - официален сайт на Apple Inc. (20.08.2018)

[7] URL: https://www.google.com/about/ - официален сайт на Google Inc. (20.08.2018)

[8] URL: https://www.microsoft.com/bg-bg - официален сайт на Microsoft (20.08.2018)

[9] URL: http://appinventor.mit.edu/explore/ - официален сайт на MIT App Inventor (20.08.2018)

Красимир Кордов, Билнур Ислям
Шуменски университет "Еп. Константин Преславски"
E-mail: krasimir.kordov@shu.bg

ANALYSIS OF HASH ALGORITHMS*

Mihaela D. Todorova

ABSTRACT: *A hash algorithm is a function that converts a data string into a numeric string output of fixed length. The output string is generally much smaller than the original data. Hash algorithms are designed to be resistant ,with hight level of security. This paper discusses some of the main properties, a study of which shows how hash function satisfies the performance requirements of security .*

KEYWORDS: *Hash Function, Statistical Analysis*

ИЗСЛЕДВАНЕ НА ХЕШИРАЩИ АЛГОРИТМИ*

Михаела Д. Тодорова

1 Въведение

Хеш функция е всеки алгоритъм, който може да се използва за преобразуване на входни данни с произволен размер, към данни с фиксиран размер. Стойностите, върнати от хеш функцията, се наричат хеш стойности, хеш кодове, извлечения или просто хешове. Криптографските хеш функции са въведени от Дифи и Хелман за употреба в инфраструктури с публични ключове [2].

Хеш функциите често се използват в комбинация с хеш таблица, често срещана структура от данните, използвана в компютърния софтуер [16], с цел бързо търсене на данни. Хеш алгоритмите, подобряват времето за търсене на информация в таблици или бази данни [3], [11], като откриват повтарящи се записи в голям файл. Те са особено полезни и в криптографията. Криптографската хеш функция позволява лесно да се провери дали дадени входни данни отговарят на съответна хеш стойност. В случаите, когато входните данни не са известни, е изключително трудно да се възстановят, като се знае единствено запазената хеш стойност.

Основните приложения на хеш функциите са за удостоверяване на съобщения и запазване на паролите [1] и целостта на данните [9]. Те се използват при работа с контролни суми, проверка на пръстови отпечатъци и при работа с кодове за коригиране на грешки. При конструирането на нови хеш функции е възможно използването на различни псевдослучайни генератори [7], [12], [13], [14], [15], [17], които да внесат допълнителна нелинейност при компресирането.

В този доклад са представени някои от основните показатели, чиито изследване изяснява дали хеш функцията е подходяща за използване в софтуерни приложения.

2 Изследване на хеш функции

Хеш функциите се характеризират с някои от следните свойства [5], [6], [10]:

*Partially supported by Scientific Research Grant RD-08-121/06.02.2018 of Konstantin Preslavski University of Shumen, Bulgaria.

- равномерно разпределение
- чувствителност
- конфузионни и дифузионни свойства и
- устойчивост по отношение на колизиите.

2.1 Анализ на разпределение на стойностите

Типично свойство на хеш-стойността е да бъде равномерно разпределена в обхвата на компресията. Имайки в предвид дължината на хеш стойността, при този тест се извършват симулационни експерименти с даден параграф от съобщението.При избраното входно съобщение се изчислява хеш стойността. Генерира се друго входно съобщение със същата дължина, състоящо се от празни интервали. След изчисляването на хеш стойността на второто съобщения, двете стойности се съпоставят и се извършва проверка дали има равномерно разпределение дори при граничните случаи. Читателят може да се запознае с примери за равномерно разпределени хеш стойности от Ref. [5], Фиг. 3 и Ref. [6], Фиг. 4.

2.2 Анализ на чувствителността спрямо оригиналното съобщение и входния ключ

Чрез този анализ се разглежда чувствителността на хеш функцията по отношение на леки промени във входното съобщение или в секретния ключ. Първата стъпка от анализа е изборът на входно съобщение и изчисляването на хеш стойността му. На базата на входното съобщение се дефинират няколко на брой нови съобщения с леки промени, след което хеш стойностите им, изчислени при същите входни параметри и условия, се сравняват с хеш стойността на оригиналното съобщение. Също така се извършва сравнение на хеш стойността, изчислена за оригиналното съобщение, при начални условия с лека промяна.

Целта на този анализ е да се покаже, че всяка малка промяна на входното съобщение или секретния ключ, води до съществена промяна на хеш стойността. Примери могат да се намерят в Ref. [5], Фиг.4 и Ref. [10], Фиг. 2.

2.3 Статистически анализ на конфузия и дифузия

От историческа гледна точка, Шанън, с публикуване през 1949 г. на неговия доклад "Теория на комуникациите в секретните системи" [4], въвежда идеята за два метода за статистически анализ на криптиращите алгоритми: конфузия и дифузия. Целта на дифузията е да се направят изходящите битове силно зависими от входните битове. В идеалния случай, малка промяна във входния блок от данни води до 50% промяна на изходния блок. Целта на конфузията е да направи връзката между входните битове и изходните битове възможно най-сложна и зависима. Този вид анализ се състои от няколко експеримента, които показват способност на хеш функцията за конфузия и дифузия. За тази цел обикновено се използват следните шест статистики:

Минимално разстояние по Хеминг: $B_{min} = min(\{B_i\}_{i=1}^{N})$

Максимално разстояние по Хеминг: $B_{max} = max(\{B_i\}_{i=1}^{N})$

Средно разстояние по Хеминг: $\bar{B} = \frac{1}{N}\sum_{i=1}^{N} B_i$

Средна вероятност: $P = \frac{\bar{B}}{n} \times 100\%$

Стандартно отклонение на броя на променените битове:

$\Delta B = \sqrt{\frac{1}{N-1}\sum_{i=1}^{N}(B_i - \bar{B})^2}$

Стандартно отклонение: $\Delta P = \sqrt{\frac{1}{N-1}\sum_{i=1}^{N}(\frac{B_i}{n} - P)^2} \times 100\%$,
където N е броя на тестовете и B_i обозначава разстоянието по Хеминг(брой различни битове) между стойностите на хеш, получени в i-тото изпитване.

Тези експерименти са разделени на два вида тестове, тестове от тип A и тестове от тип B.

При тестове от тип A, се генерира произволно съобщение, наричано оригинално съобщение, с размер L = 50n и неговата съответна n- битова стойност на хеш се изчислява. След това се генерира ново съобщение, като на случаен принцип се избира един бит от оригиналното съобщение и обръща. След това n-битовата хеш стойност на новото съобщение се сравнява с тази на оригиналното съобщение и изчисленото разстояние по Хеминг между двете хеш стойности се записват като Bi. Тази операция се повтаря N пъти, където всеки път се избира ново оригинално съобщение и един от неговите битове,избран произволно, се обръща. Тестовете обикновено се извършват със стойности за големината на хеш функцията n = 128; 160; 256; 512; 1024. Например, за 128 битови хеш стойности и $N = 10000$ е необходимо да се постигнат следните подобни резултати [8]: $B_{min} = 44$, $B_{max} = 84$, $B = 63.95$, $P(\%) = 49.96$, $\Delta B = 5.62$ и $\Delta P(\%) = 4.39$.

При тестове от тип B се генерира произволно оригинално съобщение с дължина L = 50n и съответната му n-битова хеш стойността се изчислява. След това се избира и обръща единичен случаен бит от първоначалното съобщение и се изчислява стойността на хеш функцията от модифицираното съобщение. Двете хеш стойности се сравняват и броят на променените битове се изчислява и записва като Bi. За разлика от преходния тест, в този тип тест се използва едно и също входно съобщение за всички N итерации. Тестът се извършва при стойности за големината на хеш функцията равни на n = 128, 160, 256, 512, 1024 и различни стойности на N. Например, за 128 битови хеш стойности и $N = 2048$ е необходимо да се постигнат следните подобни резултати [6]: $B_{min} = 48$, $B_{max} = 83$, $B = 64.22$, $P(\%) = 50.17$, $\Delta B = 5.65$ и $\Delta P(\%) = 4.42$.

Целта на този вид анализ е да покаже дали хеш функцията има силна способност за конфузия и дифузия и дали ще бъде надеждна срещу този вид атаки.

2.4 Тест за устойчивост на колизии

При този анализ хеш функцията се изследва въз основа на тестовете за колизии, предложени в [5]. За да се извърши количествено проучване на анализа на колизия, се извършват следните два вида тестове. При тестове от тип A се генерира входно съобщение с размер L = 50n и съответната му n-битова хеш стойност се изчислява и съхранява във формат ASCII. След това се генерира ново съобщение, като се избира случайно единичен бит от входното съобщение и се променя на 0, ако е 1 или 1, ако е 0. n-битовата хеш стойността на новото съобщение се изчислява и се съхранява в ASCII формат. Двете хеш стойности се сравняват и се преброяват ASCII символите с една и съща стойност в една и съща позиция. Освен това, абсолютната разлика D между двете хеш стойности се изчислява по следната формула

$D = \sum_{i=1}^{n/8} |dec(e_i) - dec(e_i^{'})|$,

където e_i и $e_i^{'}$ ще бъдат i-тия запис на хеш стойностите на първоначалното и модифицираното съобщение,като съответно функцията $dec()$ преобразува записите в техните еквивалентни десетични стойности.

Тестът от тип A се повтаря N = 10 000 пъти и се записват експериментите за минималната, максималната и средната стойност от D ,за различните хеш стойности с размер n = 128,

160, 256 и 512. Например, за 128 битови хеш кодове е необходимо да се постигнат подобни или по-добри от следните стойности [18]: минимална стойност 655, максимална стойност 2064 и средна стойност 1367.

При тестовете тип B се създава произволно входно съобщение с фиксиран размер L = 50n бита и се изчислява неговата съответна n-битова хеш стойност. След това се избира един бит от входното съобщение, променен на 0, ако е 1 или 1, ако е 0, и се изчислява хеш стойността на модифицираното съобщение. Експериментът се извършва за хеш стойности с размер n = 128, 160, 256 и 512, генерирани при тестове от тип B. Същото въведено съобщение се използва за всички N итерации. Например, за 128 битови хешове и $N = 6400$ е необходимо да се постигнат подобни или по-добри от следните стойности [6]: минимална стойност 661, максимална стойност 2294 и средна стойност 1360.

В допълнение към горните експерименти, тестовете на тип B се повтарят за много къси входни низове, състоящи се от един n-битов блок.

След получаване на резултатите от този вид тест се изяснява, дали хеш функцията има устойчивост по отношение на колизиите.

Следващите стъпки на екипа са конструиране на нов хеш алгоритъм базиран на някои от следните псевдослучайни генератори [12], [13], [14] и [17] и неговото изследване чрез описаните по-горе статистически тестове.

ЛИТЕРАТУРА:

[1] Eunice, A. B., Umoren, A. M., Markson, I. (2017). Design of Web-Based Customer Relation Management Application for Power Distribution Company: A Case Study of PHCN Owerri Business Unit, Mathematical and Software Engineering, 3(1), 108-123.

[2] W. Diffie, M.E. Hellman, “New directions in cryptography”, IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644-654, 1976.

[3] Jude, O. O., Jimoh, A. J., Eunice, A. B. (2016). Software for Fresnel-Kirchoff Single Knife-Edge Diffraction Loss Model, Mathematical and Software Engineering, 2(2), 76-84.

[4] C.E. Shannon, “Communication Theory of Secrecy Systems”, . Bell System Technical Journal, vol. 27, no. 4, pp. 656-715, 1949

[5] A. Kanso and M. Ghebleh, “A Fast and Efficient Chaos-Based Keyed Hash Function”, Communications in Nonlinear Science and Numerical Simulation, vol. 18, no. 1, pp. 109-123, 2013.

[6] A. Kanso and M. Ghebleh, “A Structure-Based Chaotic Hashing Scheme”, *Nonlinear Dynamics*, vol. 81, no. 1-2, pp. 27-40, 2015.

[7] Kordov, K. (2015). Signature Attractor Based Pseudorandom Generation Algorithm, Advanced Studies in Theoretical Physics, 9(6), 287-293.

[8] Z. Lin, S. Yu, and J. Lü, “A Novel Approach for Constructing One-Way Hash Function Based on a Message Block Controlled 8D Hyperchaotic Map”, *International Journal of Bifurcation and Chaos*, vol. 27, no. 7, 1750106, 2017.

[9] Nachev, A., Reapy, T. (2015). Predictive models for post-operative life expectancy after thoracic surgery. Mathematical and Software Engineering, 1(1), 1-5.

[10] H. Ren, Y. Wang, Q. Xie, and H. Yang, “A Novel Method for One-Way Hash Function Construction based on Spatiotemporal Chaos”, *Chaos, Solitons and Fractals*, vol. 42, pp. 2014-2022, 2009.

[11] Stefanov, T. (2015). System for information extraction from news sites, Mathematical and Software Engineering, 1(1), 25-30.

[12] Stoyanov, B. (2014). Self-shrinking bit generation algorithm based on feedback with carry shift register, Advanced Studies in Theoretical Physics, 8(24), 1057-1061.

[13] Stoyanov, B., Kordov, K. (2014). Novel zaslavsky map based pseudorandom bit generation scheme. Applied Mathematical Sciences, 8(178), 8883-8887.

[14] Stoyanov, B., Kordov, K. (2013) Pseudorandom Bit Generator with Parallel Implementation. In International Conference on Large-Scale Scientific Computing (pp. 557-564). Springer, Berlin, Heidelberg.

[15] Stoyanov, B., Milev, A., Nachev, A. (2010) Research on the self-shrinking 2-adic cryptographic generator. Journal of Communication and Computer, 7(11), 67-71.

[16] Stoyanov, B., Strahilov, S. (2015) Web Based Information System for Heat Supply Monitoring, Mathematical and Software Engineering, 1(2), 37-42.

[17] B. Stoyanov, K. Szczypiorski, and K. Kordov, "Yet Another Pseudorandom Number Generator", *International Journal of Electronics and Telecommunications*, vol. 63, no. 2, pp. 195-199, 2017.

[18] Y. Wang, K-W. Wong, and Di Xiao, "Parallel hash function construction based on coupled map lattices", *Communications in Nonlinear Science and Numerical Simulation*, vol. 16, pp. 2810-2821, 2011.

Михаела Тодорова
Шуменски университет "Еп. Константин Преславски"
E-mail: mihaela.todorova@shu.bg

RANSOMWARE ATTACKS AND COUNTERMEASURES

VICTORIA R. YANAKIEVA, TEODORA T. STOYANOVA

ABSTRACT: *One of the most important aspects of ensuring the security of computer systems is the identification, analysis and classification of possible threats to them. Ransomware is a malware that infects a computer device, resulting the information in its memory becoming unavailable to users. The prognosis for 2018 is that a significant increase in ransomware attacks is expected. For this reason, a number of organizations are looking for ways to deal with these growing threats.*

KEYWORDS: *Malware, Ransomware, cyberattack, WannaCry, Petya/NotPetya, BadRabbit.*

RANSOMWARE АТАКИ И ПРОТИВОДЕЙСТВИЕ*

ВИКТОРИЯ Р. ЯНАКИЕВА, ТЕОДОРА Т. СТОЯНОВА

АБСТРАКТ: *Един от най-важните аспекти на осигуряване на сигурността на компютърните системи е определянето, анализа и класификацията на възможните заплахи за тях. Ransomware е злонамерен софтуер, който заразява компютърното устройство, в резултат на което информацията в неговата памет става недостъпна за потребителите. Прогнозата за 2018 г. е, че се очаква значително увеличание на ransomware атаките. Поради тази причина, редица организации търсят начин да се справят с тези зачестили заплахи.*

1 Въведение

Целта на всяка компютърна информационна система е предоставяне на пълна, достоверна и своевременна информация. При всички информационни процеси в такива системи и мрежи в реални условия, тази информация е уязвима, както поради случайни, така и поради злонамерени дестабилизиращи фактори (заплахи), което налага да се вземат мерки за нейната защита, чрез които се постига нужното ниво на информационна сигурност [1].

Може да се приеме, че терминът информационна сигурност се отнася за състоянието на защитеност на жизнено важните интереси в информационната сфера на фирмите и хората в тях от вътрешни и външни заплахи [2].

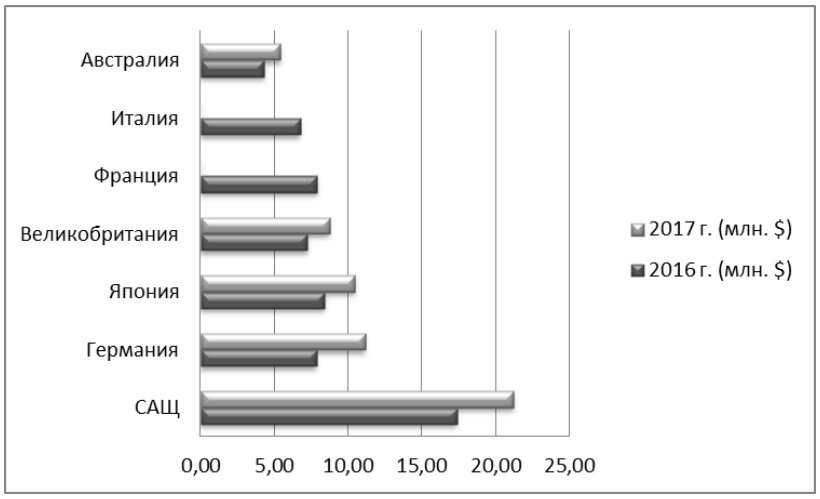
Необходимостта от защитата на различни информационни системи (частни и държавни) от външни заплахи, като изтичане на чувствителна за организацията информация, е очевидна на всички етапи от развитието на системите за защита на информацията. През последните години се обръща все по-голямо внимание на този вид заплаха поради щетите, нанасяни от нея на компаниите и организациите.

Чрез кибератаките се цели да се промени или разбие компютърна система или мрежа, която съхранява или предава дадена информация или програма.

Съгласно редовното годишно изследване на авторитетния американски институт Ponemon, на фиг. 1 се представят оценените средни разходи за престъпления в киберпространството за седем страни, включващи 254 отделни компании, през последните две години (2016-2017 г.). Компаниите в САЩ отчитат най-високата обща средна стойност, а в Австралия - най-ниската. През 2017 г. Германия бележи значително

* Настоящата статия е частично финансирана по проект № РД-08-159/09.02.2018, „Надеждност и защита на информация в социалните мрежи, графичните и 3D обекти в добавена и виртуална реалност“

увеличение на общите разходи за киберпрестъпленията (липсват данни за Италия и Франция за 2016 г.).



Фиг. 1. Средни разходи за престъпления в киберпространството за седем държави

Система за защита на информацията (СЗИ) (security system) е организирана съвкупност на всички органи, средства, методи и мероприятия, предвидени в информационна система за осигуряване на защита на информацията от разгласяване, изтичане и несанкциониран достъп към нея [3].

2 Видове заплахи

Класификацията на видовете заплахи може да бъде направена по различни критерии, но тя не е фиксирана, тъй като с развитие на техниката и технологиите се увеличават видовете заплахи [3,4]. Според природата им на произход, те могат да бъдат естествени (напр. природни явления, независещи от човека) и изкуствени (предизвикани от хората). Последните, според мотивацията на хората, се подразделят на случайни (непреднамерени) и умишлени (преднамерени), които са свързани с користни цели на субектите.

Според източника спрямо обекта на защита, заплахите са външни и вътрешни. На фиг. 2. е показана тази връзка [3].

Процентът на външните заплахи за дадена организация е много висок. Атаките могат да бъдат активни или пасивни. При активните се генерират пакети или участват в мрежата, докато при пасивна атака се подслушва мрежата или се проследяват потребителите [5].

От външните преднамерени заплахи - злонамерените атаки се извършват чрез прикачени файлове към имейл или чрез посещение на подозрителни заразени уебсайтове. Като някой от най-често срещаните видове заплахи са:

- *Spyware*

Този типове злонамерен софтуер остава скрит, докато събира ценна информация. Достатъчно е да се деинсталира, за да бъде премахнат от компютъра.

- Trojan horse (Троянски кон)

Злонамереният софтуер тип „троянски кон“ заразява компютъра, най-често маскиран като антивирусен софтуер или компютърна игра.

- *Drive-by-downloads*

Злонамереният код е вграден предимно в новинарски уебсайтове и след посещение на страницата започва сканиране на компютъра за уязвимости в сигурността, т.е. остарели приложения, плъгини за браузъри, приложения за чат и т.н.

- *Botnet*

След заразяване със злонамерен код, чрез интернет компютъра се свързва с контролен компютър. Най-уязвим софтуер са браузърите, Adobe Flash, Adobe Reader и Java. Актуализирането на приложенията може да блокира 65% от атакуващите вектори.

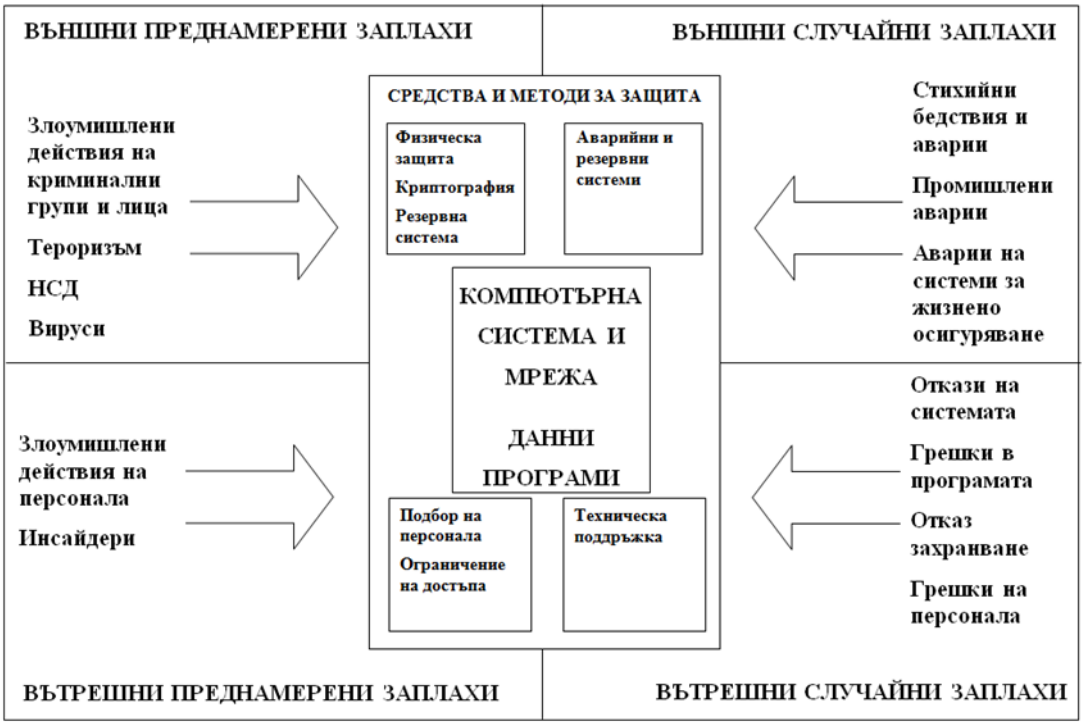
- *Adware*

Adware често се изтегля заедно с безплатните програми. Той е злонамерен софтуер, използван за проследяване на онлайн поведението на заразения потребител.

- *Ransomware*

Най-разпространените видове ransomware криптират всички или някои от данните на компютъра и след това изискват голямо плащане (откуп), за да се възстанови достъпа до данните. Този тип злонамерен софтуер е предпочитан, до голяма степен благодарение на криптовалутата Bitcoin [5,6,7].

Съществуват редица други видове злонамерен софтуер, но настоящата статия се фокусира върху актуалните през последните три години ransomware заплахи [8].



Фиг. 2. Връзка на заплахите с обекта на защита

3 Ransomware атаки

Според доклад на Verizon за разследване на пробиви и изтичане на данни за 2017 г., ransomware е петата най-разпространена форма на злонамерен софтуер през 2016 г., издигайки се от позиция 22 през 2014 г. Всъщност от 2016 г. насам са се появили над 200 нови вида ransomware.

Най-засегнатите страни от 1 април до 3 октомври 2017 г са: САЩ (17,2%), Великобритания (11,1%), Белгия (8,6%) и т.н. [9]

Ransomware атаките са значително по-бързи и по-евтини за изпълнение в сравнение с много други кибер заплахи, и имат много по-висока печалба.

Предимствата на ransomware злонамерен софтуер са:

• По-лесно е да се изпрати криптовалута, отколкото традиционните пари.

• По-малко хора участват в операцията, от където следва, че хакерите имат по-голяма печалба.

Има няколко различни начина, по които хакерите избират организациите, към които да приложат ransomware атака. В повечето случаи се насочват към университетите, защото те са с по-малка защита и различна потребителска база, което улеснява проникването в защитата им.

Държавни агенции, адвокатски кантори или медицински центрове са предпочитани от хакерите, защото е по-вероятно бързо да платят откуп тъй като, се нуждаят от незабавен достъп до файловете си [10].

Анализът на Check Point показва, че през 2015 г. ransomware атаките причиняват щети от 325 милиона долара. За следващата година атаките са се увеличили 15 пъти, струвайки 5 милиарда долара [11].

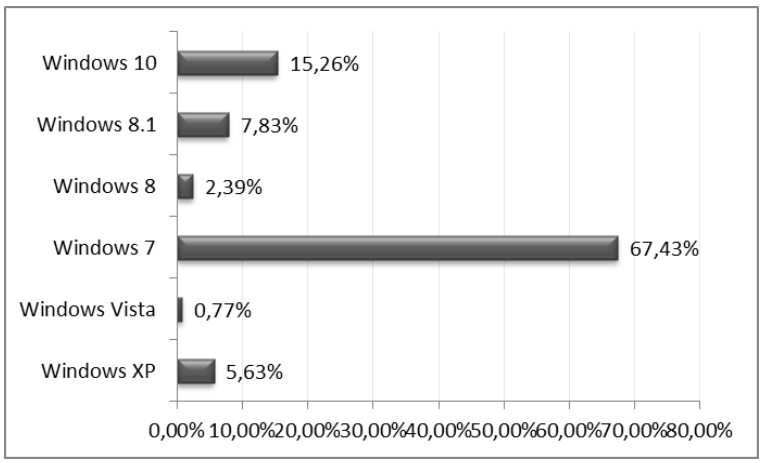
Най-актуалните през последните две години ransomware атаки са WannaCry, Petya/NotPetya и BadRabbit.

3.1 WannaCry

WannaCry е зловреден софтуер създаден през май 2017 г., с вероятен произход Северна Корея. Познат е като WanaCrypt, Wana Crypt0r и Wana Decrypt0r. Използва EternalBlue exploit, откраднат от хакерите The Shadow Brokers от американската агенция за национална сигурност, и причинява щети на летища, банки, университети, болници и др. Разпространява се в около 150 страни по света, главно Русия, Украйна, САЩ и Индия. За възстановяване на файловете е необходимо плащане с Bitcoin криптовалута, като при просрочване на даденото време от 72 часа цената се удвоява. Седем дни след заразяване със злонамереният софтуер следва изтриване на файловете от компютъра. WannaCry сканира за TCP и UDP портове 139 и 445 (SMB) от компютрите [11].

Данните от Kaspersky показаха, че по-голямата част от инфектираните с WannaCry компютри са с операционна система Windows 7, показано на фиг. 3.

WannaCry представлява 45,3% от всички ransomware атаки.



Фиг. 3. Съотношение на версиите на операционна система Windows, засегнати от WannaCry

3.2 Petya/NotPetya

Petya е ransomware софтуер, който заразява целевия компютър, криптира някои от данните в него и извежда на екрана съобщение, обясняващо как може да се плати в Bitcoin, за да получат ключовете, нужни за декриптиране на данните. В първоначалния вариант на зловреден софтуер Petya, която започна да се разпространява през март 2016 г., достига компютъра на жертвата, прикрепен към имейл. Представлява пакет с два файла: изображение и изпълним файл, често с "PDF" в името на файла. След кликване върху този файл и приемане на предупреждението за Windows User Access Control, Petya рестаритира компютъра и инсталира свой собствен зареждащ скрипт. Файлове са в компютъра и не са шифровани, но жертвата няма достъп до частта от файловата система, която указва къде са. В този момент хакерите изискват плащане в Bitcoin, за да декриптират твърдия диск.

През юни 2017 г. се създава подобрена версия на злонамерения софтуер Petya, наречен NotPetya, разпространяващ се бързо, като засегнатите сайтове са фокусирани в Украйна, но се появяват както в Европа, така и извън нея. Новият вариант бързо се разпространява от компютър на компютър и от мрежа в мрежа, без да изисква спам имейли или социално инженерство, за да получи административен достъп. Въпреки, че е разновидност на Petya, NotPetya не попада в графата ransomware вируси [12,13]. NotPetya има някои допълнителни правомощия, които според експертите по сигурността го правят по-опасен от WannaCry.

3.3 BadRabbit

BadRabbit се разпространява чрез фалшиви актуализации на Flash, идващи от компрометирани популярни домейни. Той е сравнително нов ransomware софтуер и споделя 13% от своя код с този на Petya, но ключовите криптиращи функции се обработват от легитимен инструмент за криптиране (DiskCryptor). За разлика от NotPetya, BadRabbit използва уникални Bitcoin портфейли за всяка жертва.

Според данните, представени от ESET по време на актуализирането, 65% от жертвите днес са в Русия, следвани от Украйна (12,2%), България (10,2%), Турция (6,4%) и Япония (3,8%) [14].

4 Противодействие

Има инструменти, специално разработени за борба с ransomware. Проектът No More Ransom - основан през 2016 г. от холандската полиция, Европол EC3, Kaspersky и McAfee и в партньорство с над 100 други организации по целия свят, помогна за декриптирането на 28 000 устройства и обхваща над 100 вида ransomware.

С цел защита на данните фирмите създаващи софтуер добават в настройките опция, включваща:

- Автоматично запазване на копие на базата с данни – директорията може да бъде друг дял на диска, USB памет, виртуално устройство или мрежов адрес.
- E-mail адрес за изпращане на резервните копия на базата данни.

Има няколко действия, чрез които да се противодейства и заплахата да бъде избегната:

- Архивиране на актуални данни.

Стандартното архивиране, което позволява защита от загуба на данни много често не е сигурно, защото хакерите получили достъп до служебни акаунти биха могли да си присвоят архивираната информация. Решението на подобен проблем е използването на

специфични криптографски алгоритми (собствено проектирани) с цел допълнителна защита на информацията на дадена организация [15,16].

• Използване на антивирусен софтуер с добра репутация.

Важен фактор е добрата антивирусна, но и тя не е решение на проблема. Нужно е една малка промяна в кода на ransomware вируса, за да остане неоткриваем. Необходимо е редовно обновяване на антивирусния софтуер.

• Актуализация на операционната система на компютъра [10].

Установено е, че над 50% от системите, засегнати от атаките на ransomware, работят с остаряла операционна система - Windows 7. Необходима е актуализация на операционната система или използването на операционна система като Linux, която е практически неуязвима за вируси.

• Обучение на служителите за правилна кибер-хигиена

Задаване на ясни правила за отваряне на e-mail връзки и прикачени файлове. Забрана за посещаване на несвързани със служебните задължения на служителите сайтове.

• Подсигуряване на мрежата

Изграждане на защитна стена, блокираща достъпа до уязвими портове и услуги в локалната мрежа. Имплементиране в защитната стена на организацията на филтри за уеб съдържание, блокиращи ненадеждни и доказано компрометирани домейни. Имплементиране в mail сървъра на организацията на централизиран, редовно актуализиращ се антивирусен софтуер, сканиращ всяко e-mail съобщение за известните към момента злонамерени кодове.

• Изграждане на навици у обикновения потребител

Честа грешка е инсталиране на неизвестен софтуер или даване на администраторски права. Препоръчително е избягването на посещенията на съмнителни сайтове.

5 Заключение

В този доклад става ясно, че броят на засегнатите потребители и щетите от ransomware атаки ще нараства. Посочените по-горе подходи за превенция на атаките са добра отправна точка в борбата с тези кибер заплахи. Спазването им значително ще ограничи риска и ще гарантира цялостност и сигурност на данните на всеки потребител и организация.

Повечето атаки от този вид засягат потребителите на Windows, но хората не са имунизирани при използването на други платформи, включително мобилни устройства.

ЛИТЕРАТУРА:

[1] Христов, Хр., Сигурност на фирмата и противодействие на посегателствата срещу нея. Университетско издателство „Епископ Константин Преславски“, монография, Шумен (2014). ISBN: 978-954-577-981-7.

[2] Zhelezov, S., Paraskevov, H., Hristov, H., Boyanov, P., Uzunova, B., An architecture of steganological subsystem for information protection. Proceedings of 10-th International Conference ICBBM, Liepaya, Latvia, (2014), 123-128.

[3] Железов, С., Оценка на ефективността на системи за защита на информацията в компютърните системи. Университетско издателство „Епископ Константин Преславски“, дисертация, Шумен (2014).

[4] Станев, С., Железов, С., Компютърна и мрежова сигурност. Университетско издателство „Епископ Константин Преславски”, Шумен (2005). ISBN 954-577-306-5.

[5] Kadir, A. F., Stakhanova, N., Ghorbani, A. A., Understanding Android Financial Malware Attacks: Taxonomy, Characterization, and Challenges. University of New Brunswick (2018).

[6] Asamoah-Okyere, E., The changing face of cybercrime: How mobile devices have changed the approach to committing cybercrime, MSc, University of Strathclyde (2014).

[7] Agrawal, M., Singh, H., Gour, N., Kumar, A., Evaluation on Malware Analysis. International Journal of Computer Science and Information Technologies, 5 (3) (2014), 3381-3383.

[8] Vijayalakshmi, Y., Natarajan, N., Manimegalai, P., Babu, S. S., Study on Emerging Trends in Malware Variants. International Journal of Pure and Applied Mathematics, 116 (22) (2017), 479-489.

[9] Brenner, B., 2018 Malware Forecast: ransomware hits hard, continues to evolve. Sophos, 11 февруари 2017. <https://news.sophos.com/en-us/2017/11/02/2018-malware-forecast-ransomware-hits-hard-crosses-platforms/> (10.07.2018).

[10] Fruhlinger, J., What is ransomware? How it works and how to remove it. CSO, 13 ноември 2017. <https://www.csoonline.com/article/3236183/ransomware/what-is-ransomware-how-it-works-and-how-to-remove-it.html> (15.07.2018).

[11] Seals, T., One Year After WannaCry: A Fundamentally Changed Threat Landscape. Threatpost, 17 май 2018. <https://threatpost.com/one-year-after-wannacry-a-fundamentally-changed-threat-landscape/132047/> (16.07.2018).

[12] Fruhlinger, J., Petya ransomware and NotPetya malware: What you need to know now. CSO, 17 октомври 2017. <https://www.csoonline.com/article/3233210/ ransomware/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html> (17.07.2018).

[13] Fox-Brewster, T., Petya Or NotPetya: Why The Latest Ransomware Is Deadlier Than WannaCry. Forbes, 27 юни 2017. <https://www.forbes.com/sites/ thomasbrewster/2017/06/27/petya-notpetya-ransomware-is-more-powerful-than-wannacry/#c556f3d532e9> (17.07.2018).

[14] Ragan, S., BadRabbit ransomware attacks multiple media outlets. CSO, 24 октромври 2017. <https://www.csoonline.com/article/3234691/security/badrabbit-ransomware-attacks-multiple-media-outlets.html> (20.07.2018).

[15] Kordov, K., Modified pseudo-random bit generation scheme based on two circle maps and XOR function. Applied Mathematical Sciences, 9 (3) (2015), 129-135.

[16] Kordov, K., Signature Attractor Based Pseudorandom Generation Algorithm. Advanced Studies in Theoretical Physics, 9 (6) (2015), 287 – 293.

Теодора Тихомирова Стоянова
Шуменски университет „Еп. Константин Преславски“
E-mail: t.stoyanova@shu.bg

Виктория Росенова Янакиева
Шуменски университет „Еп. Константин Преславски“
E-mail: v.yanakieva@shu.bg

MODERN STGANOGRAPHIC APPROACHES IN SOCIAL NETWORKS

HRISTO I. PARASKEVOV, ALEKSANDAR Y. STEFANOV

ABSTRACT: *Online social networks (OSN) have gained great popularity among Internet users because of the opportunities they provide for easy sharing of news, opinions, multimedia content and various kinds of activities. In this regard, the OSN has become an important factor in the formation of positions and attitudes in modern society. Logical is the reaction of some governments and organizations both to using the abovementioned qualities of social networks and to make efforts to censor them. Two interrelated issues become more and more relevant: the development of steganographic methods using the OSN's specificities to overcome imposed censorship, and the creation of a set of measures to perform adequate stealth analysis to reveal built-in secret, malicious communication channels.*

KEYWORDS: *steganography, social networks, hiding data*

СЪВРЕМЕННИ СТЕГАНОГРАФСКИ ПОДХОДИ В СОЦИАЛНИТЕ МРЕЖИ*

ХРИСТО И. ПАРАСКЕВОВ, АЛЕКСАНДЪР Й. СТЕФАНОВ

1 Въведение

Социалните мрежи предоставят множество и разнообразни възможности за изграждане на стеганографски тайни канали. Важни моменти са огромният брой потребители и съответстващия обем на обменяната информация. Подходите при реализирането на стеганографски канали могат да се разгледат в две основни направления:

✓ методи експлоатиращи спецификите на OSN при публикуване и обмен на съдържание;

✓ методи използващи спецификите на OSN при отразяване на поведението на потребителите.

Следва да се отбележи, че е налице и трета възможност – разработване на хибридни методи, комбиниращи наличните възможности както по съдържание, така и по поведение. В настоящата статия е направен обзор на съществуващи към момента подходи и възможности за използване на стеганография в онлайн социални мрежи.

Едни от най-масово използваните стеганографски контейнери са графичните изображения. Известни са множество методи, приложими към различни графични формати, позволяващи получаване на добри резултати [1]. Графичните изображения са основна част от публикуваната в онлайн социалните мрежи потребителска информация. В тази връзка е логично да се проучи приложимостта на гореспоменатите методи в тази среда. Проведените изследвания обаче показват, че част от онлайн социалните мрежи са въвели ограничения относно поддържаните от тях графични формати. Нещо повече честа

* Докладът е частично финансиран със средства от проект РД-08-159/09.02.2018

практика е извършването на обработка на публикуваните от потребителя изображения. Съгласно резултатите публикувани в [2], прилаганите политики се различават значително за различните платформи: например Google+ не обработва изображенията ако резолюцията им не надвишава 2048x2048, в тази връзка използването на всеки графичен стеганографски инструмент е допустимо. При Twitter ситуацията е по-различна - заличават се някои от полетата, съдържащи метаданни, което прави неприложими методите, които ги експлоатират. Същевременно интегритета на изображения по-малки от 1024x768 се запазва. Подобно на Twitter Facebook премахва метаданните от изображението, освен това обаче го подлага на допълнителни обработки - модификация на размера, стойностите на част пикселите, компресията. Всичко това води до сериозни предизвикателства по отношение използването на графична стеганография в тази социална мрежа. Публикуваните в [3] резултати кореспондират с направените по-горе наблюдения. Въпреки ограниченията налагани от Facebook, в резултат на проведени изследвания, публикувани в [4] е установено, че при избор на подходящ контейнер, графичната стеганография е приложима и в тази социална мрежа. Най-добри резултати в това отношение са постигнати със специализирания софтуер JP Hide & Seek (JPHS) - до 60 % успеваемост, като положителни резултати са постигнати и с Steg и Steghide.

2 Стеганографски подходи в социалните мрежи

Перспективен подход за приложение на стеганографията в социалните мрежи е описан в [5]. Реализираният метод е наречен StegHash и използва наличния в множество социални мрежи елемент наречен hashtag. Под hashtag се разбира обикновено етикет състоящ се от дума, предхождана от символа "#". Обикновено се "прикача" към публикация (снимка, видео, текст) като показва нейната относимост към дадена тематика. Особено полезен е в социални мрежи, в които е налице ограничение в дължината на публикуваните текстови съобщения.

Описаният метод, разширява възможностите на използването на графични изображения, видеофайлове и др. като контейнери на тайното съобщение. Добавянето на хаштагове към такива обекти позволява изграждане на връзки между тях, увеличавайки многократно размера на скритото съобщение. На всеки набор от n на брой хаштага, съответстват n! на брой пермутации, които са индивидуални индекси на всяко съобщение. Притежателите на секретния ключ (паролата), които разполагат със секретния генератор (функцията) могат да изградят връзка между тези индекси и в последствие да проследят веригата между отделните контейнери, съдържащи отделните части на тайното съобщение [5]. Методът е реализиран в две от популярните онлайн социални мрежи Twitter и Instagram, като са отчетени особеностите им по отношение на прилаганата към публикуваните изображения обработка. Установено е, че различните платформи имат различен подход по отношение възможностите за извършване на търсене по прикрепените към обекта (контейнера) хаштагове - докато Twitter няма ограничения по отношение на броя им, в Instagram се допуска търсене само по един. При експериментите е използван малък набор от хаштагове (3,4,5,6) с оглед избягването на нарушаване на работата на социалната мрежа посредством генериране на солиден допълнителен трафик, което би провокирало активирането на съответните политики на сигурност. Регистрирани са обнадеждаващи резултати за малки по обем съобщение (100% успеваемост) като за по-големи е необходимо да се извършат допълнителни оптимизации.

Едно от приложенията на стеганографията в социалните мрежи е насочено към осигуряване на защита на персоналните данни, предоставени от потребителя в неговия

профил. В [6] е описана система за такава защита означена като NOYB (none of your bussiness). При регистрирането и използването на онлайн социална мрежа потребителят в общия случай първоначално въвежда и периодично допълва и коригира, голямо количество лична информация - име, адрес, месторабота, семейни връзки, снимков материал. Тази информация става достъпна за определен от потребителя кръг от хора, в съответствие с възприетата и прилагана от социалната мрежа политика за сигурност. Масово използваната социална мрежа Facebook например, изисква потребителят да използва същото име, което използва и в ежедневието си, както и да посочва точна информация за себе [7]. В тази връзка при спазване на тези изисквания потребителят посочва достоверна информация, която обаче би могла да стане достояние на не съвсем добронамерени лица. Информацията може да бъде използвана както за извършване на измами така и за осъществяване на определени политически и бизнес цели. Широко известен е скандалът със събирането и обработването на лични данни на Facebook потребители от Cambridge Analytica. Посредством приложението "thisisyourdigitiallife" [8] организацията автоматизирано е събирала и обработвала персонална информация за изграждане на "психографичен" профил на повече от 87 милиона потребители [9]. Според твърденията на представители на компанията събраната информация може с висока точност да предскаже високочувствителна лична информация като: сексуална ориентация, етническа принадлежност, религиозни и политически възгледи, ниво на интелигентност, използване на психоактивни вещества, емоционален статус, възраст и пол [8]. В тази връзка е обяснимо защо част от потребителите предпочитат да се регистрират под фалшива самоличност и да посочват неверни данни в контактната си информация. Разбира се при установяването на този факт от страна на Facebook, потребителите са заплашени от закриване на профилите им. В предложената в [6] система NOYB персоналната информация се разделя на "атоми". Всеки от тях може да се криптира, като по този начин информацията става достъпна само за запознатите с ключа и алгоритъма на криптиране. Разбира се повечето от социалните мрежи не биха толерирали директно въвеждане на криптирани данни. Тук на помощ идва стеганографията. Посредством предварително генериран речник се извършва замяна на отделните "атоми" на реалните потребителските данни със съответните им стойности в речника, генериран на псевдослучаен принцип. Например потребителските данни (име, пол, възраст) - (Алис, Ж, 25) се разделят на два "атома" - (Алис, Ж) и (25). Първият "атом" се заменя с (Боб, М), а вторият с (28). Така за масовия потребител профилът принадлежи на Боб, 28 годишен мъж, а за "просветените" е ясно, че се касае за Алис, 25 годишна жена. Посредством този подход се реализират няколко цели:

✓ защита на личните данни - за масовия потребител остава в тайна истинската самоличност на ползвателя на защитения профил;

✓ защитата може да се реализира без да е необходимо съдействие от страна на онлайн социалната платформа. Същевременно ако политиката на администраторите на социалната мрежа е да оказват съдействие, защитата може да се приложи към всички потребители;

✓ системата е трудно разкриваема дори за враждебно настроена платформа, особено в случаите на социална мрежа с голям брой потребители. За разкриването ѝ е необходимо анализиране на немалък брой "заподозрени" профили с цел откриване на данни уличаващи потребителя в използване на неистинска идентичност.

Разбира се гореописания подход има и своите недостатъци. Част от потребителските данни не могат да бъдат заменени с фиктивни, поради факта, че трябва да бъдат уникални

и се използват за обратна връзка при регистрацията. Това в особена сила важи за телефонния номер и адреса на електронната поща.

Друг възможен подход за реализиране на стеганографски канал е използването на популярната в онлайн социалните мрежи възможност за реакция на потребител по отношение на достъпни за него публикации [10]. В този случай се реализира таен канал въз основа на поведението на потребителя. Носител на тайната информация могат да бъдат поставени "лайкове" (харесвания) на определени публикации. Предложеният подход може да бъде разширен като в реализирането на канала участват: време (както астрономическо така и относително), на поставяне на реакциите, поредност на реакциите (за множество статии), тип ("харесване", "любов", "ха-ха", "Еха", "тъга", "гняв"). Допълнително разширяване на канала може да се постигне посредством менажиране на множество профили от страна на изпращача на тайното съобщение, при което се манипулират поредността, времената и типовете на реакциите на контролираните от него профили. Реакциите могат да бъдат както по отношение на публикации на получателя на тайното съобщение, така и по отношение на публикации на трета, неутрална към комуникацията страна.

По отношение на споделената текстова информация под формата на публикации и разменената такава в чат комуникация например би могла да се използва текстова стеганография. Основна трудност при нея е липсата на излишък от информация, какъвто е налице при графичните и звуковите файлове. [11] Един обикновен текстов документ (например .txt формат) се записва, обработва и възпроизвежда от компютърната система във вид идентичен или много близък до това, което се изобразява пред погледа на потребителя. По-перспективни в това отношение са файлови формати поддържащи форматиране на текста - шрифт, размер, отместване, разстояние между редове и символи.

Методите приложими в текстовата стеганография могат да бъдат разделени на две основни групи:

- ✓ манипулация на форматирането на текста;
- ✓ манипулиране на значението на текста.

Методите от втората група имат своите ограничения [11]:

- синтактичен - поставяне или пропускане на синтактични знаци (, . : ; и др.) на съответните места в текста. Количеството информация, което може да бъде скрито по този начин е в пряка връзка с броя на знаците и в тази връзка като цяло е силно ограничено). Съответно неправилното поставяне на голям брой излишни знаци би събудило основателни подозрения за наличието на целенасочено манипулиране на текста;

- семантичен - използване на синоними на определени думи, от предварително договорен речник, с цел предаване на скрита информация:

Логическа "0"	Логическа "1"
Голям	Значителен
Студен	Хладен
Хубав	Красив
Мотор	Двигател

Предвид наличието на нюанси в значението на отделните думи от синонимната двойка, са налице ситуации, при които директната замяна на едната дума с другата е не винаги удачна - например в словосъчетанието "големи усилия" замяната със значителен е възможна - "значителни усилия". Не така стои въпросът при "голяма сграда", в случая по-

подходяща била алтернативата "огромна сграда", а не "значителна сграда". В тази връзка при създаването на речници би следвало да се отчитат гореспоменатите особености, което от своя страна би се изразило в усложняване на структурата на речника (например добавяне на алтернативни думи в двете колони).

Логическа "0"	Логическа "1"
Голям, важен	Огромен, значителен

- използване на абревиатури или съкращения. В ежедневието си често използваме абревиатури като алтернатива на пълното изписване на наименования (Шуменски университет - ШУ; мобилен телефон - GSM и др.). Подобна е ситуацията с използването на съкращения при провеждане на чат комуникация "не знам" се замяна често с "нзн" или "nz", "какво правиш" с "к пр". Аналогично при е и при англоезичните чатове - "be right back" с "brb", "face to face" с "F2F" и т.н. Подобно на семантичния метод използването на пълното наименование или съкращението (абревиатурата) може се експлоатира за предаване на скрито съобщение. Количеството информация и в този случай е ограничено по обем. Тук отново е налице необходимостта от предварително договаряне на речници между двете страни.

- Начин на изписване на думите (спелуване) - при този метод се използва обстоятелството, че едни и същи думи в английския език се изписват по различен начин в Британския и Американския варианти на езика.

AmericanSpelling	BritishSpelling
Favorite	Favourite
Criticize	Criticise
Fulfill	Fulfil
Center	centre

И в този случай количеството информация, което може да бъде скрито е малко поради малкия брой думи, отговарящи на горното условие.

- Генериране на правописни грешки в текста - предвид публикуването в социалните мрежи на разнообразна информация от широк кръг от потребители с различна степен на грамотност е налице възможност да се реализира таен канал посредством преднамерено и контролирано допускане на правописни грешки в публикацията или кореспонденцията. Откриването на подобен канал би изисквало изучаване и анализ на проявената от потребителя езикова грамотност с цел преценка дали се касае за неволно или целенасочено допускане на съответните езикови грешки.

Въпреки ограниченията по отношения на реализирания посредством гореописаните методи таен канал, те са директно приложими както при публикуване на текстова информация в потребителския профил така и при осъществяване на чат комуникация между двама и повече потребители.

По-перспективни по отношение на капацитета на тайния канал са методите на текстова стеганография използващи манипулиране на форматирането на текста:

- ✓ промяна на разстоянието между редовете;
- ✓ промяна на разстоянието между буквите;
- ✓ добавяне на празни интервали между буквите;

✓ използване на емотикони - на различните емотикони съответстват различни стойности ":-)" - "0", ":-(" - "1", ":-*" - "01", ":-P" - "10" и т.н. [12];

Следва да се отбележи, че за разлика от последните два от гореописаните методи, първия и втория не са директно приложими при публикуване на текст в профила или чат комуникация. За да се използват е необходимо обработения текст да бъде записан във формат, поддържащ осъществените манипулации (например .doc или .docx) и изпратен като файл до друг потребител.

Друга възможност за използване на текстова стеганография е генерирането и последващо разпращане или публикуване на спам съобщения. В самото съобщение могат да бъдат приложени методи, манипулиращи както значението така и форматирането на текста. Предвид огромния брой спам съобщения циркулиращи в Интернет в това число и социалните мрежи (например "Ако не разпратиш това съобщение на n на брой потребители в следващия m на брой часа, ще се случи ..." предхождано от някаква история/информация) е налице възможност за реализиране на таен канал с немалък капацитет, особено при комбиниране на няколко метода.

Прилагането на криптографски алгоритми повишава устойчивостта на стеганографските методи[13, 14].

3 Заключение

Описаните подходи и методи дават основание да се счита, че при използването на социални мрежи могат да се реализират перспективни стеганографски канали. Усилията могат да бъдат насочени към създаване на хибриден метод, при който скритото съобщение се вгражда в контейнер с голям капацитет (графично изображение, видео или звуков файл), намиращ се на подходящо място в Интернет пространството (сайтове за видео споделяне, облачни структури за съхранение на информация и др.). Същевременно другият важен компонент – стегоключа се предава между заинтересуваните страни при използване на набор (матрица) от профили, посредством контролирано и синхронизирано въздействие върху поведението им – лайкване на публикация (време, поредност, тип), споделяне на публикация (време, поредност, местоположение, достъпност), активиране и деактивиране на комуникационно приложение, добавяне и премахване на потребители в списъка, манипулиране на публикувани или изпращани текстови съобщения и др. За реализирането на такъв метод е необходимо:

✓ извършване на проучване на достатъчен брой социални мрежи, комуникационни програми, сайтове за видео споделяне;

✓ избор на подходящи социална мрежа, комуникатор(и), сайт(ове) за видео споделяне;

✓ генериране на необходимия брой потребителски профили;

✓ изпълване с подходящо съдържание на профилите;

✓ провеждане на съответните експерименти с цел определяне оптимален контейнер за съобщението и метод за предаване на стегоключа.

Важен момент при експлоатирането на стеганографски методи в социални мрежи е своевременното реагиране и пренастройване на метода съобразно динамиката във функционалността на използваната среда.

ЛИТЕРАТУРА:

[1] Станев, Ст. Стеганологична защита на информацията. Шумен: Университетско издателство „Еп. К. Преславски“, 2013. ISBN: 978-954-577-825-4.

[2] N. ‚Jianxia, I. Singh, Harsha V. Madhyastha, Srikanth V. Krishnamurthy, Guohong Caox, and Prasant Mohapatra. Secret Message Sharing Using Online Social Media

[3] Еминов Д., С. Хасанова, Д. Тончев - Стеганография в онлайн социални мрежи – MATTEX, 2014, том I, стр.173-179

[4] D. Tejas, J. Hiney, Using Facebook for Image Steganography

[5] Szczypiorski, K, StegHash: New Method for Information Hiding in Open Social Networks

[6] Guha S., K. Tang, P. Francis - NOYB: Privacy in Online Social Networks

[7] Facebook Inc. Условия за ползване – "https://web.facebook.com/terms.php?_rdc=1&_rdr", 20 юли 2018 г.

[8] Sanders, J. and D. Patterson, Facebook data privacy scandal: A cheat sheet. https://www.techrepublic.com/article/facebook-data-privacy-scandal-a-cheat-sheet/, 21 юли 2018 г.

[9] Whittaker, Z. Facebook: Cambridge Analytica took a lot more data than first thought. https://www.zdnet.com/article/facebook-confirms-cambridge-analytica-took-more-data-than-first-thought/, 20 юли 2018 г.

[10] Zhang X., - Behavior steganography in social network

[11] Roy S., M. Manasmita - A Novel Approach to Format Based Text Steganography

[12] Chandragiri A., P. Cooper, Y. Liu and Q. Liu - Implementing Secure Communication on Short Text Messaging

[13] Kordov, K., Stoyanov, B., (2017), Least Signi cant Bit Steganography using Hitzl-Zele Chaotic Map, International Journal of Electronics and Telecommunications, 63(4), 417-422. doi: https://doi.org/10.1515/eletel-2017-0061

[14] Stoyanov, B., Zhelezov, S, Kordov, K., (2016), Least signi cant bit image steganography algorithm based on chaotic rotation equations, Comptes rendus de l'Acad emie bulgare des Sciences, 69(7), 845-850.

Христо Иванов Параскевов
Шуменски университет „Епископ Константин Преславски“,
E-mail: h.paraskevov@shu.bg

Александър Йонков Стефанов
Шуменски университет „Епископ Константин Преславски“,
E-mail: a.stefanov@shu.bg - докторант

DESIGN AND CONSTRUCTION OF A VIRTUAL COMPUTER MODEL

STOYAN V. STOYANOV, STANIMIR K. ZHELEZOV

ABSTRACT: *The purpose of this work is to build a virtual model of a computer system for student education, based on analysis of different platforms, creating virtual reality and its related 3D graphics. An classification of three-dimensional models was made. Software platforms for three-dimensional modeling and creation of virtual scenes have been analyzed and selected. A virtual model has been built.*

KEYWORDS: *Virtual reality, 3D – modeling, virtual scenes.*

ПРОЕКТИРАНЕ И ИЗГРАЖДАНЕ НА ВИРТУАЛЕН МОДЕЛ НА КОМПЮТЪРНА СИСТЕМА*

СТОЯН В. СТОЯНОВ, СТАНИМИР К. ЖЕЛЕЗОВ

АБСТРАКТ *Целта на настоящата разработка е на базата на анализ на различни платформи, за създаване на виртуална реалност и свързаните с нея 3D графики, да се създаде виртуален модел на компютърна система за обучение на студенти. Направена е класификация на тримерните модели. Анализирани са и са избрани софтуерни платформи за тримерно моделиране и създаване на виртуални сцени. Разработен е виртуален модел.*

1 Въведение

Целта на настоящата разработка е на базата на анализ на различни платформи, за създаване на виртуална реалност и свързаните с нея 3D графики, да се създаде виртуален модел за обучение на студенти по дисциплините „Асемблиране на компютри“ и „Компютърни архитектури“. За тази цел е необходимо да се решат следните задачи:

- Да се направи анализ на софтуерните системи за 3D компютърна графика и виртуално моделиране;
- На базата на анализа на най-популярните инструменти за 3D моделиране и създаване на виртуална реалност да се избере подходящ инструментариум;
- Да се разработи приложение за нуждите на обучението.

2 Моделиране на 3D обекти

Всяко триизмерно изображение, създадено от компютър, изисква три основни компонента:

1. Описание на триизмерна сцена;
2. Един или повече източници на светлина
3. Описание на камерата или изглед към сцената.

Описанието на сцената обикновено се състои от един или повече модели или триизмерни структури. Обикновено един човек мисли за модел като самостоятелна част, например молив или дърво, а сцената като сглобяване на тези части в пълна триизмерна среда. Това отношение повлиява най-често срещаната процедура за изграждането на

* Настоящата статия е частично финансирана по проект № РД-08-159/09.02.2018 “Надеждност и защита на информация в социалните мрежи, графичните и 3D обекти в добавена и виртуална реалност” на ШУ

триизмерна сцена: изграждат се много модели и след това се сглобяват. Всеки модел има две описания[1]:

- математическо представяне на структурата на формата.
- изглед на формата при осветяване.

Структурното описание е основно геометрия. То ни казва къде е обектът в пространството и къде не е. Повечето компютърни програми използват вградената изчислителна система в днешните компютри. Този хардуер е с много висока, но ограничена прецизност. Някои методи за моделиране са много близки до този подход; те създават точки в пространството или го нарязват много фино и му слагат етикет празно или пълно. Други методи се опитват да позволят да се опише модела по-абстрактно, като например, че една чаша представлява цилиндър с дъно.

Другата част от всеки модел е описанието на повърхността. Това се свежда до описване физиката на взаимодействието на повърхността на модела със светлината. За щастие се оказва, че тази физика се ръководи от няколко описателни термини, които имат интуитивно значение за човека, като цвят, блясък и прозрачност[2].

Тъй като моделите често симулират форми от реалния свят, трябва да се определи колко подробен да бъде моделът [3,4].

За да бъдат анализирани и сравнени съществуващите програми за 3D моделиране е необходимо да се разгледат видовете модели, които се реализират от софтуерните системи.

Класификация на моделите

Повърхностни и гранични модели

Най-простият модел на повърхност е просто колекция от 3D точки. Те могат да бъдат организирани в прост списък или могат да бъдат по-добре структурирани като контури, части или секции. Повърхностите, представени от точки, изискват доста гъсто разпределение на точките за точно моделиране.

Импулсни повърхности / алгебрични уравнения

Тези повърхности са определени като решения за алгебрични формули. Един познат клас от такива повърхности са квадратичните обекти. По принцип повърхността е решение на уравнение като $F(x, y, z) = 0$.

Полигони

Полигоналните (полиедрични) модели са едно от най-често срещаните представяния в компютърната графика. Моделите се дефинират като мрежи от полигони, образуващи триизмерни полихедри. Всеки полигон (примитив) се състои от някои свързани върха, ръба и лицевата структура. Възможни са различни структури от данни[8]. Групи полигони се съхраняват в списъци, таблици или свързани структури. Полигоните са оразмерени, оформени и позиционирани така, че да покрият напълно необходимата повърхност на определена резолюция. Многоъгълните модели са относително лесни за дефиниране, манипулиране и показване. Те са най-разпространеният модел, обработен от хардуер и софтуер за графичен дизайн на работната станция. По принцип полигоните са най-добри при моделирането на обекти, които имат плоски повърхности.

Извити повърхности

Тъй като полигоните са добри при представянето им на повърхности, са изразходвани значителни усилия за определяне на математическите формули за действително извити повърхности. Всяка извита повърхност се нарича пластир; пластирите могат да бъдат съединени по техните гранични ръбове в по-сложни повърхности. Обикновено пластирите се дефинират от полиноми от нисък ред

(обикновено кубични), които дават на пластира лесно изчислителни математически свойства, като добре дефинирани повърхностни нормали и допирателни и изчислими условия на непрекъснатост между периферните съседни пластири. Съществуват многобройни формули на извити повърхности, включително: Безие, Хермайт, полиноми, рационални полиноми, кардинални сплайни, композитни спланове и др.

Обем и CSG модели

Първият обемен модел, който се разглежда, е моделът на воксела. Тук пространството е напълно запълнено с мозайка от кубчета или паралелепипеди, наречени „voxels“ (обемни елементи). Обикновено има плътност или друга цифрова стойност, свързани с всеки воксел. Съхраняването на мозайка с висока разделителна способност е скъпо в пространството, но не струва нищо в структурата на данните (просто голям триизмерен масив от стойности). Обикновено някои схеми за оптимизиране на съхранението са необходими за подробна работа (1K x 1K x 1K пространства)[5].

Осмични дървета

Осмичните дървета са една от структурите за данни, използвани за обемни модели, които се натрупва в дадено триизмерно пространство. Оригиналният обем, например куб, е разделен на 8 кубчета, ако не е празен. Рекурсивно, всеки под-куб е разделен, когато не е празен, докато не достигне някакъв елемент с минимален размер. Тъй като празните кубчета не са подразделени, ефективността на пространството за съхранение се увеличава. Основното използване на осмичните дървета изглежда е схема за индексиране на ефективността на достъпа в голям триизмерен масив.

Конструктивна геометрия

Една от най-ефективните и мощни техники за моделиране е конструктивната геометрия. За разлика от схемите на воксел и осмичните дървета, няма изискване редовно да се натрупва цялото пространство. Освен това примитивните обекти не се ограничават до кубове; съществуват множество прости примитиви като куб, сфера, цилиндър, конус, половин пространство и т.н. Всеки примитив се трансформира или деформира и се позиционира в пространството. Комбинациите от примитиви или от предишни комбинирани обекти се създават от булевите операции. Следователно обектът съществува като дървовидна структура, която се оценява по време на рендиране или измерване[6].

Специализирани (единични примитивни) системи

Общата структура на метода на конструктивната геометрия с нейните множество примитивни обекти и скъп и бавен метод ray-tracing често се намалява, за да се спечели ефективност при конструкцията на модела, да се избегнат булеви комбинации, различни от обединението, и да се увеличи скоростта на показване. Идеята е да се ограничат примитивите до един тип, а след това да се проектират манипулации и характеризират алгоритми, за да се възползва от еднаквостта на представянето.

Потенциални функции

Интересно обобщение на модела на сферата е обмислянето на обема като потенциална функция с централна и полева функция, която намалява монотонно (чрез експоненциална или полиномна функция) от центъра навън. Няма "радиус" или размер на потенциалната функция; по-скоро, размерът или повърхността се определя чрез задаване на прагова стойност за полето. Това, което прави това по-интересно, е, че потенциалните функции действат като енергийни източници: прилежащите потенциални функции имат припокриващи се полета и получената стойност в дадена точка в пространството е всъщност сумата от активните полета в тази точка. По този начин съседните полета се смесват гладко, за разлика от "гънките", които се получават с фиксирани радиусни сфери.

Системи от частици

Обобщавайки сферите в различна посока, системите за частици намаляват сферата до нулев радиус. Обемът се характеризира с набор от (обикновено движещи се) частици, които индиректно определят пространството. Всяка частица има свой цвят, път, история и времетраене. Тяхното движение обикновено се контролира от вероятностни алгоритми. Системите от частици са използвани за моделиране на огън, газове, експлозии, фойерверки и тревисти полета[7].

Има няколко типа програми, които да помогнат създаването на триизмерни модели. Интерактивен софтуер – един клас на програма за моделиране интерактивен, когато обикновено дизайнерът седи пред терминал с клавиатура и мишка и манипулира форми на екрана.

- Интерактивните моделиращи софтуери обикновено съдържат разнообразни помощни средства за проектиране, които помагат да се постигне известна точност в модела: често срещан пример е да се "snap"(вмъкват) точки на модел в точки на друг модел или към невидима решетка. Моделите се изграждат чрез интерактивно избиране, модифициране и сглобяване на примеси на примитиви.
- Скриптов софтуер - друг клас на програма за моделиране разчита на входния скрипт за дефиниране на модела. Скрипта определя формите в модела една по една, като идентифицира всяка от тях с примитива и параметрите и, които определят този модел.
- Друг софтуер - Съществуват и други начини за създаване на модели, например чрез дигитализиране на съществуващи триизмерни структури или чрез анализ на снимки.

Тези програми обикновено се наричат моделиращи и съчетават в себе си различни типове моделиране от посочените в класификацията. Една идея, която е обща за повечето софтуери, е, че дизайнерът може да създаде копие на някаква основна форма (като блок или кръпка) и след това да я модифицира, за да създаде част от модела. Основните форми се наричат примитиви за тази програма. Прототипната форма е идеалната и случаите са практични реализации на този идеал [6].

3 Избор на софтуер и реализация на 3D модела

При избора на софтуер за изграждане на необходимия за виртуализацията на компютърната конфигурация 3D модел бяха анализирани най-разпространените софтуерни системи за 3D моделиране - Cinema 4D, Blender, 3ds Max, Maya и CAD/CAM [8].

Всяка от разгледаните системи притежава редица предимства като мощен анимационен пакет, поддръжка на широк формат за импортиране и експортиране, богат списък от инструменти за моделиране и др. Естествено те притежават и множество недостатъци - слаба система от частици, недостатъчна интуитивност, забавяне при високо детайлни модели, лошо организиран интерфейс и др. Някои от тези системи имат голям набор от инструменти и готови вградени обекти, но при тях се наблюдават недостатъци като висока цена, огромни изисквания към хардуера, стръмна крива на изучаване и др. От друга страна безплатните софтуери са бедни от към вградени инструменти и обекти, държат се доста нестабилно, забавят работата си при по-детайлни модели и т.н.

От направените анализи на софтуерните системи за 3D моделиране като най-подходяща се откроява Cinema 4D [9]. Някои от основните и предимства пред останалите са:

• Изчистен интерфейс: Персонализируемите плаващи и конфигурируеми панели за наблюдение позволяват пространството да бъде посветено на произведението, а не на интерфейса.

• Cinema 4D е известна със своята достъпност. Лесна за използване от артисти и дизайнери, както и от потребители без технически познания в областта.

• Mograph е невероятен набор от инструменти в Cinema 4D, който ускорява процеса на създаване на анимации и графики за движение.

• Новоразработен кеш за излъчване (Irradiance Cache).

• Актуализиран инструмент Bevel.

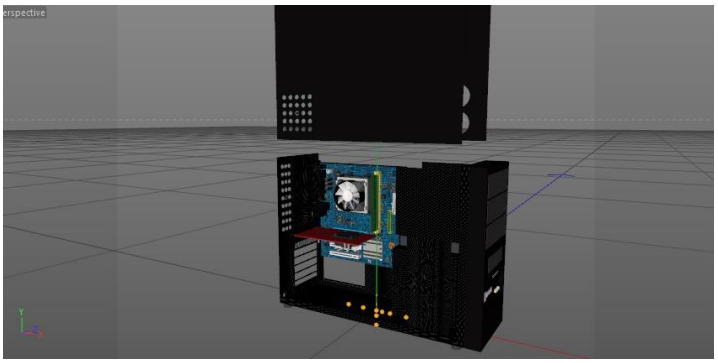
• Intel Embree във физически рендерер.

• Изключително стабилна.

• Cinema 4D е напълно заредена с богата библиотека от предварително зададени обекти.

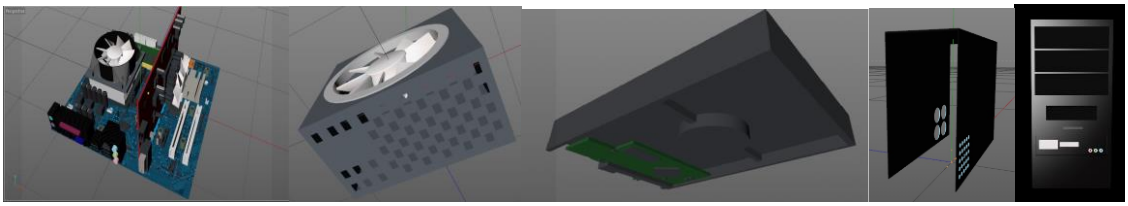
Cinema 4D е интуитивен, удобен както за професионални дизайнери така и за начинаещи. Изключително голям набор от функции и инструменти, с които времето за моделирането на обекта е значително по-кратко. Тя предоставя изчерпателна документация, в която е дадено пълно описание, предоставено от редица примери, както и видео и текстови уроци и сесии за обучение на живо. Също така предоставя „friendly“ интерфейс с което позволява лесно изграждане на тримерните модели. Не на последно място програмата предоставя възможност за лесно премоделиране на обектите с цел по-лесно изграждане на алтернативни тримерни обекти, което е една от целите на настоящата разработка от гледна точка на бъдещо развитие.

За реализацията на 3D модела на компютърната система (фиг. 1) се изграждат модели на основните елементи на системата – дънна платка, захранване, твърд диск и кутия (фиг. 2).

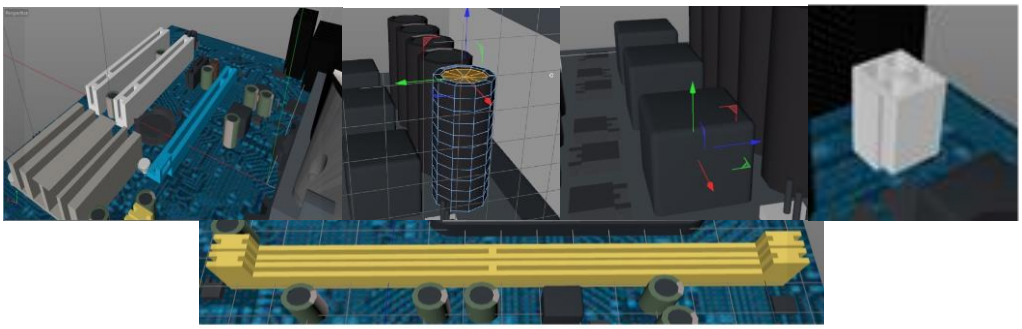


фиг. 1 Триизмерен модел на персонален компютър

За създаването на основните обекти се използват допълнителни подобекти (техни наследници), които са съставни части на обекта, и текстуриране на обекта. Дънната платка представлява съвкупност от различни видове слотове (фиг. 3) и разположените върху тези слотове компоненти – видеокарта, процесор, оперативна памет, охладители и др.(фиг. 4). А също така и различни дребни детайли – кондензатори и др.(фиг. 3)

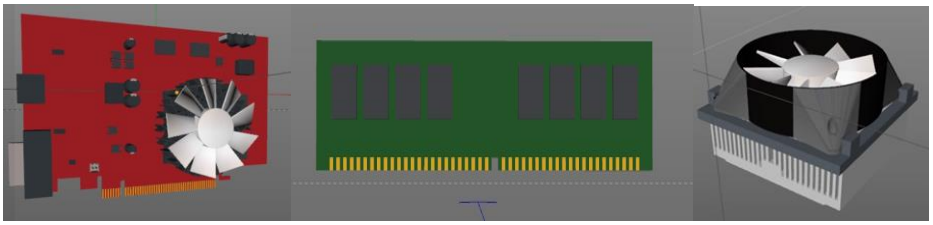


фиг. 2 Основни елементи на модела



фиг. 3 Основни елементи на модела на дънната платка

Всеки от тези компоненти може да се разглежда и като самостоятелен обект. Това позволява при моделиране на допълнителен набор от компоненти да се променя конфигурацията на компютърната система. По този начин може да се увеличи броя на конфигурациите, които да се предложат на обучаемите.



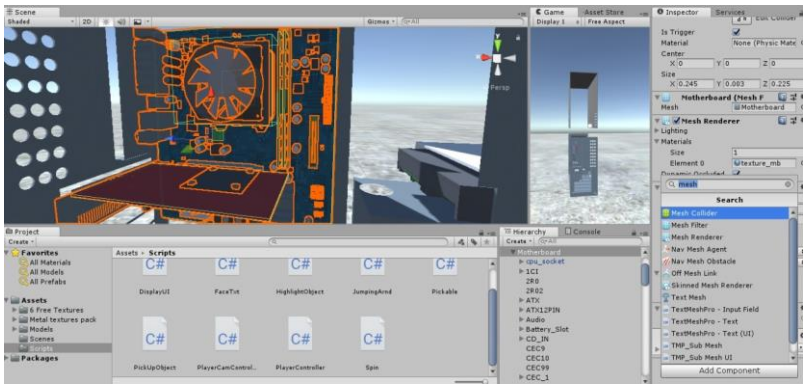
фиг. 4 Компоненти на компютърната система

4 Реализация на приложение за виртуална реалност

След успешното моделиране на обекта е ред на неговото импортиране във виртуалната реалност. Както и при избора на среда за моделиране е направен сравнителен анализ на различни софтуерни платформи за виртуализация. Сравнени са предимствата и недостатъците на най-разпространените продукти – Unity и Unreal Engine. За да бъде реализирана виртуалната сцена е избрана софтуерната платформа Unity [10]. Нейните предимства като отличен баланс на лекота на използване и мощност, вграден физически базиран рендеринг и висококачествени графични ефекти, активното развитие, редовно фиксирани бъгове и редовно пускани нови функции и т.н., определят нейния избор за реализиране на виртуалната сцена.

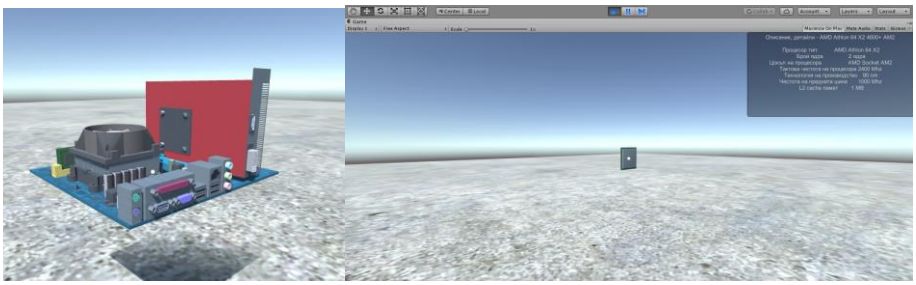
Крайната цел на приложението е асемблирането и деасемблирането на компютърна конфигурация във виртуална среда. За целта се експортира на модела от Cinema4D към

Unity и с помощта на вградените инструменти на Unity се импортира в програмата, като се запазва детайлността на тримерния модел. След успешното експортиране/импортиране отделните компоненти на модела да се „създадат“ като движещи се обекти за да може играча да ги вдига и оставя на различни позиции. На всички основни обекти на модела (капак, дънна платка, хард диск, захранващ блок, процесор, охладителя на процесора, РАМ паметта) се добавя по един нов компонент с име Mesh Collider (фиг. 5). Меш колизията се използва при сложни обекти с неточна форма, тя автоматично заема формата на обекта.



фиг. 5 Mesh collider върху компонентите на компютъра, тоест те вече могат да си взаимодействат с околната виртуална среда.

Модела и неговите подобекти се нуждаят от меш колизия за да може да бъдат вдигани, оставяни и т.н., в противен случай без колизията моделът би бил статичен. За да може отделните обекти на модела да се вдигат, оставят или въртят се създава C# скрипт. Чрез добавяне на функция в вече създадения скрипт се добавя информация към всеки обект, който е бил избран (фиг. 6).



фиг. 6 Дънната платка и процесора след изваждането и добавената информация

5 Заключение

Изучаването на учебни дисциплини с хардуерна насоченост, като „Компютърни архитектури“ и „Асемблиране“, предполага наличието на голям обем технически средства и ресурси. Тяхното представяне на студентите като хардуерни компоненти води до чисто практически затруднения от гледна точка на създаването на помещения и хранилища на този вид нагледни материали. За да се избегнат посочените неудобства могат да се използват възможностите на системите за изграждане на виртуална реалност.

Разработените виртуална сцена и свързания с нея тримерен модел могат да послужат като добра основа за последващото изграждане на цялостни виртуални системи за асемблиране и деасемблиране на компютри. С помощта на тези системи студентите биха могли, независимо от местоположението си, да получат необходимите им знания и умения за апаратната част на различни видове компютърни системи и техните параметри, характеристики и съвместимост. Предложеният тримерен модел лесно може да бъде модифициран с цел разширяването базата от компоненти за визуализиране и по този начин да се представи развитието на компютърната техника през годините с нагледни средства. Това е позволява настоящата разработка да се разглежда като първи етап от изграждането на цялостна система за виртуално обучение в областта на информационните технологии и хардуер.

ЛИТЕРАТУРА:

[1] Haresh Khemani, Applications of CAD Software: What is Solid Modeling? www.brighthubengineering.com, 2008г.

[2] Wisslar, Virginia. Illuminated pixels: the why, what, and how of digital lighting. Cengage Learning, 2013.

[3] Gahan, Andrew. 3D Automotive Modeling: An Insider's Guide to 3D Car Modeling and Design for Games and Film. Focal Press, 2012.

[4] Vaughan, William. Digital modeling. New Riders, 2011.

[5] Straßer, Wolfgang, and Hans-Peter Seidel, eds. Theory and practice of geometric modeling. Springer Science & Business Media, 2012.Masjukov, A.V., Masjukov, V.V., Multiscale modification of Shepard's method for multivariate interpolation of scattered data. In: Mathematical Modeling and Analysis. Proceeding of the 10th International Conference MMA2005&CMAM2, 467-472.

[6] KANA, Martiale G. ZEBAZE. "Introduction to solid modeling.", 1988.

[7] Savelonas, Michalis A., Ioannis Pratikakis, and Konstantinos Sfikas. "An overview of partial 3D object retrieval methodologies." Multimedia Tools and Applications 74.24 (2015): 11783-11808.

[8] Earnshaw, Rae A., ed. Virtual reality systems. Academic press, 2014.

[9] Kaminar, Aaron. Instant Cinema 4D Starter. Packt Publishing Ltd, 2013.

[10] Roedavan, Rickman. "Unity Tutorial Game Engine." Bandung: Informatika 2014.

Стоян Василев Стоянов
Шуменски Университет „Еп. Константин Преславски“
E-mail: 404i90@gmail.com

Станимир Кунчев Железов
Шуменски Университет „Еп. Константин Преславски“
E-mail: s.zhelezov@shu.bg